ホワイトペーパー：
モバイルデバイスの管理に
電子証明書が欠かせない理由とは？

モバイルデバイスの管理に電子証明書が欠かせない理由とは？

本書の概要

このホワイトペーパーでは、急速に企業での導入が進むスマートフォンやタブレット PC などのモバイルデバイスの管理に必要な、認証セキュリティについて解説します。様々な事例を詳しく検討すると、市場に出回っている多様なモバイルデバイス向けのセキュリティクレデンシャル（認証情報）には電子証明書が最適であることが分かります。Symantec Managed PKI Service がなぜモバイルデバイス向けの電子証明書の管理に最適なのかを MDM と証明書の導入事例を交えながらご紹介します。

Confidence in a connected world. Symantec.

モバイルデバイスの管理に電子証明書が欠かせない理由とは？

目次

モバイルデバイスの管理に電子証明書が欠かせない理由とは？

はじめに

生産性の向上や新たなビジネスシーンへの活用を目的に、スマートフォンやタブレットPCといったモバイルデバイスのビジネス利用が増加しており、モバイルデバイスが企業のITツールとして欠かせない要素となっていることはもはや疑う余地がありません。

しかし、様々な形態のモバイルデバイスの登場があまりにも急速であるため、IT部門が考慮しなければいけない管理の範囲も広がっており、変化にしっかりと対応しなければ、セキュリティの脆弱性に付け込まれて個人情報の盗難やなりすましなど、セキュリティリスクが増加することが懸念されます。もはや企業はファイアウォールに囲まれたPCだけを管理すればいいのではありません。モバイルデータやアプリケーションを保護することはもちろんのこと、モバイルデバイスの利用者自体が信頼できるかどうかも重要となります。

モバイルデバイスの管理と信頼できるかどうかが重要

デスクトップPCが中心だった時代には、IT部門はハードウェアおよびソフトウェアの標準構成を定義することで、サポートを容易にし、メンテナンスコストを削減し、共通のプラットフォームでセキュリティ上の脅威に対抗してきました。その後、さまざまなエンタープライズソフトウェア管理ツールを用いて、デスクトップPC上のソフトウェアや設定、セキュリティポリシーすべてをリモートで集中管理するようになりました。

当然のことながら、IT部門はモバイルデバイスに関しても、これまでと同様にデバイス構成を制御し、クライアントのソフトウェアの配布や監視を行い、脆弱性を最小限に押さえ、データのリスクを制御したいと考えているでしょう。また、モバイルデバイスはその形状から、社外に持ち出す機会も多いため、紛失や盗難のリスクが高く、これまで以上に適切な管理を行う実装を必要としていると思います。

こうしたニーズに対応するため、様々なソフトウェアやサービス、Mobile Device Management (MDM) が登場しており、遠隔からのデバイスのプロビジョニングやデバイスの追跡、アプリケーションの管理、デバイスへのポリシーの適用といった機能や、社外のデバイスをリモートワイプしたり、無効化したりする機能が提供されています。モバイルデバイスの導入には、企業の重要なリソースを守るため、これまでと同等の厳重な管理を行い、ネットワークの延長線上としてデバイスを信頼する必要があります。

モバイルデバイスの信頼性の確保

モバイルデバイスのセキュリティの確保は、管理さえしていれば大丈夫というわけでは必ずしもありません。モバイルデバイスを安全に利用するには、管理機能に加え、適切な認証が必要です。
セキュリティ担当者の大半は、MDMを導入していても、ユーザ名とパスワードによる認証だけでは、企業のIT資産を守る上で強固さに欠けると感じています。パスワードのみによる認証では、パスワードの弱点を回避するセキュリティ対策として「ユーザに頻繁にパスワード変更を実施」する方策では、ユーザがパスワードを忘れないよう書き留めてしまうなどの問題も少なくありません。

IT管理において強固なセキュリティを実現するには、企業のネットワークやアプリケーションにアクセスするデバイスが信頼できるかどうかを特定できる、強固なセキュリティクレデンシャルが必要です。強固なセキュリティクレデンシャルは、ユーザを特定できるのみならず、デバイスを検証して安全に情報を転送できます。セキュリティクレデンシャルにはいくつかの形態がありますが、要件を満たすクレデンシャルのなかで最も幅広く利用されているのが、電子証明書です。

電子証明書のメリット

電子証明書は、ネットワークやデータの安全性を確保してきた20年近くにわたる実績があります。公開鍵暗号技術に基づいているため、パスワードだけの認証よりもはるかに安全で、強固な認証を実現できます。しかも、デバイスの認証やメールの暗号化以外に、ウェブサイトやVPNの認証、ワイヤレスネットワークなどの保護にも活用できるなど、幅広い用途に利用が可能なことがメリットです。電子証明書がこれほど幅広く認められ、採用されているのは、単一のクレデンシャルによって企業のさまざまな認証セキュリティ要件をサポートできるからです。

電子証明書は、Apple iOS®やAndroidといった、モバイルPCやタブレットPC、スマートフォンのオペレーティングシステム (OS) で広くサポートされています。また、多くのエンタープライズネットワーク アプリケーションやソフトウェアアプリケーションでもサポートされています。

次の図は、モバイルデバイスで電子証明書を使用する主なアプリケーションの例を示したものです。

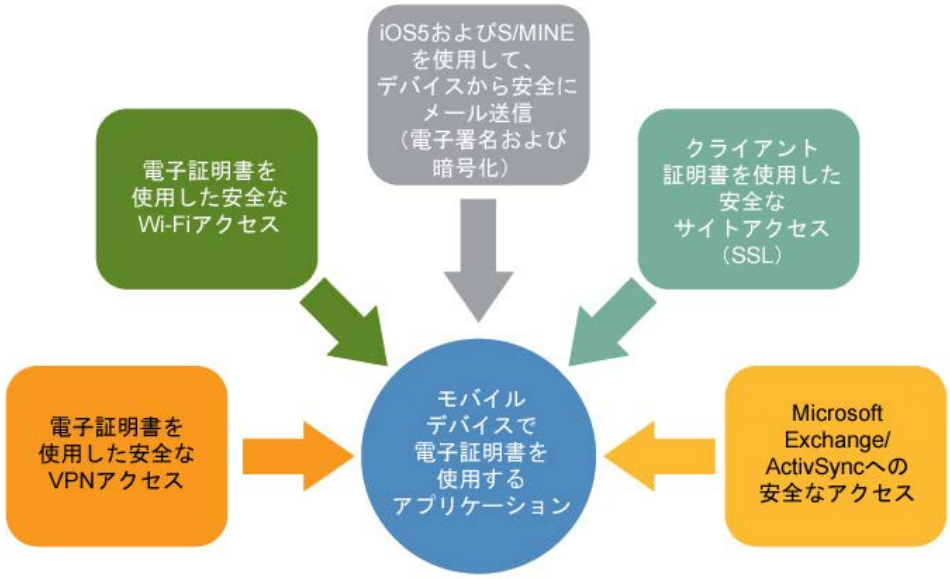

図1：様々なエンタープライズアプリケーションに対応可能な電子証明書

モバイルデバイスではキーボードのスペースが限られているため、ユーザ名とパスワードを入力しなくてもよい電子証明書は操作面でも優れており、30日、60日、90日ごとにパスワードを変更する必要もないため利便性が高いのも特徴です。アプリケーション向けに個別に構成しない限り人の介在が不要なため非常に透過性が高い理想的な認証方法です。

さらに、電子証明書はほぼすべてのエンタープライズ向けのMDMソリューションで広くサポートされています。MDMでは電子証明書の利用は必須ではありませんが、電子証明書を使用しないと、デバイス認証やデバイス検証のための通信（たとえばプロファイルの転送）が安全ではない方法で行われる可能性があります。電子証明を利用しない場合、単なるユーザ名/パスワードであっても、単一デバイスに対応付けられないワンタイムパスワードであっても、デバイスのプロファイルを他のデバイスで復元することが可能な場合があるほか、企業のリソースへのアクセスに利用するクレデンシャルが暗号化されずに平文で含まれている可能性があります。したがって、より強固なセキュリティを実現するには、MDMと電子証明書を組み合わせて利用し、プロファイルを安全に転送および保護することが必要です。これはApple社のドキュメントで規定しているプロファイルを安全に配信および保護するためのプロトコルで、公開鍵基盤（PKI）が使われていることでも、電子証明書の利用がいかに重要かお分かりいただけると思います（PKIでは電子証明書を使用します）。

企業は、モバイルデバイス向けのセキュリティ対策としてMDMと電子証明書を利用したデバイス認証の他に、電子メールの暗号化・署名、VPN認証、Wi-Fi認証などの利用用途にも電子証明書を利用すれば、より対投資効果を高めることもできます。

企業での電子証明書の管理と導入

モバイルデバイスのアプリケーション内部で証明書をサポートしている場合もありますが、IT部門は、デバイス上に安全に証明書を配布したり、必要に応じて証明書の更新や失効を行ったりなど、証明書のライフサイクルを効率的に管理する必要があります。次の図は、証明書ライフサイクル管理に含まれる様々なプロセスを示しています。

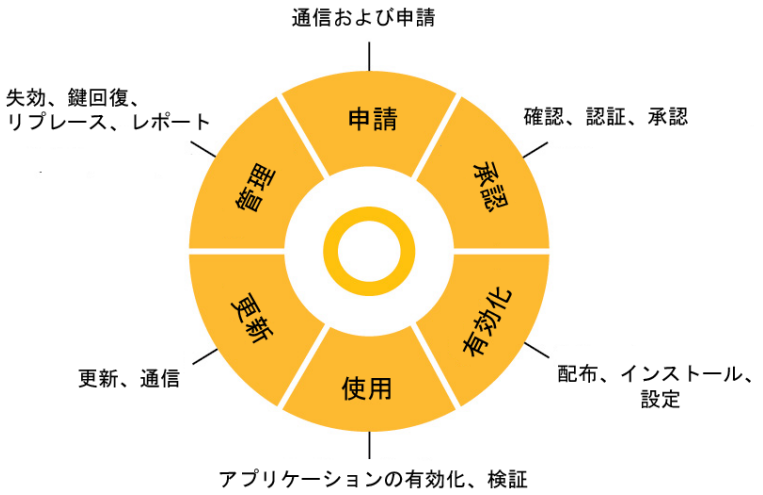

図2：証明書ライフサイクル管理の重要なプロセス

公開鍵暗号方式に基づく電子証明書を管理するには、公開鍵基盤（PKI）が必要です。PKIの主な機能は、ユーザやデバイスに証明書（および関連する公開鍵）を正確かつ確実に配布し、証明書のライフサイクルを管理することにあります。こうした重要な機能を実現しようとする場合、企業はインハウス型でPKIソフトウェアを導入するか、クラウド型で外部の信頼できるプロバイダにPKIの構築・運用を委託するかを選択する必要があります。自社での導入を決めた場合、MDMの有無にかかわらず、PKIを導入してモバイルデバイスを管理できるようにするには、カスタマイズを行う必要があります。

PKI導入における最も一般的な選択肢は、次のとおりです。

- IT部門のスタッフが管理とサポートを行う、OpenCA™やEnterprise Java Bean Certificate Authority（EJBCA）といったオープンソースソフトウェアツール
- 基本的なPKIツールが含まれる、Microsoft Active Directory®証明書サービスなどの市販ソフトウェア
- すぐに利用可能なマネージドサービスとして提供される、Symantec Managed PKI Serviceなどのクラウドベースの PKIソリューション

企業のPKI導入の成功の鍵は、使いやすさと管理のしやすさ、そしてユーザの操作性です。さらに、世界中の様々なアプリケーションやデバイスにクレデンシャルの利用を展開した場合、そのニーズに合わせた拡張ができるかどうかも重要なポイントです。

次表に示す成功要因を考慮し、企業のニーズや利用可能なリソースに合致したPKIソリューションを選択する必要があります。

適切な実装 選択肢	クラウド型 PKI : ホスティングによる PKI プラットフォームを利用	インハウス型 PKI : 既製または市販の PKI ソフトウェアを利用
PKI 機能	グローバルな信頼のルートと検証サービスを持つ、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、長年の運用実績を持つ確かなソリューション。	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。
導入の容易さ	広く普及している企業向けウェブブラウザ、電子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すべてサポート。一般的なアプリケーションに関しては、環境の大部分を事前プロビジョニング。管理ポータルの高度なテンプレート化により、導入が容易。	高頻度で、大幅なカスタマイズやプロフェッショナルサービスによるサポートが必要。多くの場合、クロスプラットフォームのサポートは限定的か、独自のクライアントソフトウェアが必要。
自動化	iOS Over-the-Air（OTA）や Microsoft Auto-Enrollment といったクライアント自動化プロトコルのサポートにより、シンプルかつ透過的にユーザやデバイスを申請可能。証明書をユーザデバイスに配信する際に、手作業での構成は不要。	大半のオンプレミス PKI ソリューションには、自動化機能はほとんど、あるいはまったくない。たとえば、Microsoft 証明書サービスでサポートされるのは Windows Mobile デバイスへの直接発行のみ。
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。高い拡張性。耐障害性に優れた高キャパシティの基盤を活用。	基盤、冗長性、災害復旧といったサービスすべてを企業側が準備。企業は可用性と拡張性の要件に自ら対応。
セキュリティおよびリスク管理	業界をリードする、熟練した鍵管理/証明書プラクティス。米国国防総省や Adobe CDS などのために、運用やポリシーの認証を外部で監査。	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	シマンテックのセキュリティプロフェッショナルは、厳しい審査と高度なトレーニングを受けている。こうしたプロフェッショナルは、セキュリティと PKI に関する最新の知識とスキルを維持。	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。 経験不足や人員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	オンラインでの申請、検証、管理サービスを実現する、パブリック認証局（CA）の完全なポートフォリオ。 企業は、プライベートまたはパブリックのトラストネットワーク（世界最大）を選択可能。	企業側がカスタムソリューションを 100%構築。自己署名証明書による、自社管理のプライベートシステムでは、社内アプリケーションしか信頼されない。相互認証や検証は社内に限定。

Symantec Managed PKI Serviceでシンプルな管理とコストの削減を実現

クラウド型のマネージドサービスであるSymantec Managed PKI Serviceは、あらゆる規模の企業のモバイルデバイスやMDM環境へ容易に証明書を導入できます。Symantec Managed PKI Serviceはクラウドベースのサービスのため、PKIの運用に関わるソフトウェア/ハードウェアインフラストラクチャはシマンテックがホスティングします。企業は複雑なPKIの構築をシマンテックにアウトソースして手間を削減できるほか、システムやソフトウェアの保守が不要になるため、運用経費を削減できます。Symantec Managed PKI Serviceが実現しているグローバルでの展開、厳密なファシリティ、高可用性（HA）、および災害復旧（DR）を各企業が自社で実現するとしたら、おそらく莫大な費用がかかるでしょう。

シマンテックはインターネットセキュリティとPKIサービス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PKIサービスプラットフォームを構築しています。20年近くにわたる豊富な運用実績で蓄積したノウハウとセキュリティおよびデータセンターのエキスパートにより、企業のモバイルデバイスの導入を支援します。

Symantec Managed PKI Serviceによる運用メリット

モバイルデバイス向けの認証強化にSymantec Managed PKI Serviceを導入すると、次のような3つの運用上のメリットが得られます。

1. **MDMとの組み合わせ：多様な導入モデルから選択が可能**
   Symantec Managed PKI Serviceは、グローバルで展開されているSymantec™ Mobile Management、MobileIron®、AirWatch®、Fiberlink®、Zenprise®や、国内で展開されているCLOMO、MobiConnectといった多数のMDMソリューションとウェブサービスインターフェイスを通じて統合いただけます。企業は自社のニーズに対応したソリューションを幅広い導入モデルから選択いただけます。
2. **容易な証明書の管理**
   Symantec Managed PKI Serviceでは、事前にプロビジョニングされたウェブベースの環境が提供されますので、モバイルデバイスへの証明書を発行するための設定や、ユーザ申請、証明書承認、証明書検証といった証明書の管理も容易に行えます。
3. **モバイルプラットフォームアプリケーションとの統合**
   Symantec Managed PKI Serviceは、iOSやAndroidなどの主要なモバイルプラットフォームとの高度な統合機能を提供します。これによりお客様は、MDMを導入していなくても、クライアントデバイスやアプリケーションの構成を自動化できます。

Symantec Managed PKI Serviceを利用することにより、証明書の申請、配信、インストールがいかにシンプルに行え、様々なモバイルデバイスの利用においてメリットを得られるか、２つのモデルをご紹介しながら解説します。

MDMでオペレーションを行うモデル

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（Symantec Managed PKI Service）の仲介役として機能します。証明書は、アプリケーションもしくはセキュアデータの一部として処理され、MDMを用いてデバイス上で管理します。次の図のようにMDMサーバが証明書の発行を申請し、取得した証明書や関連する構成を、それぞれの構成に基づいてモバイルデバイスにインストールします。

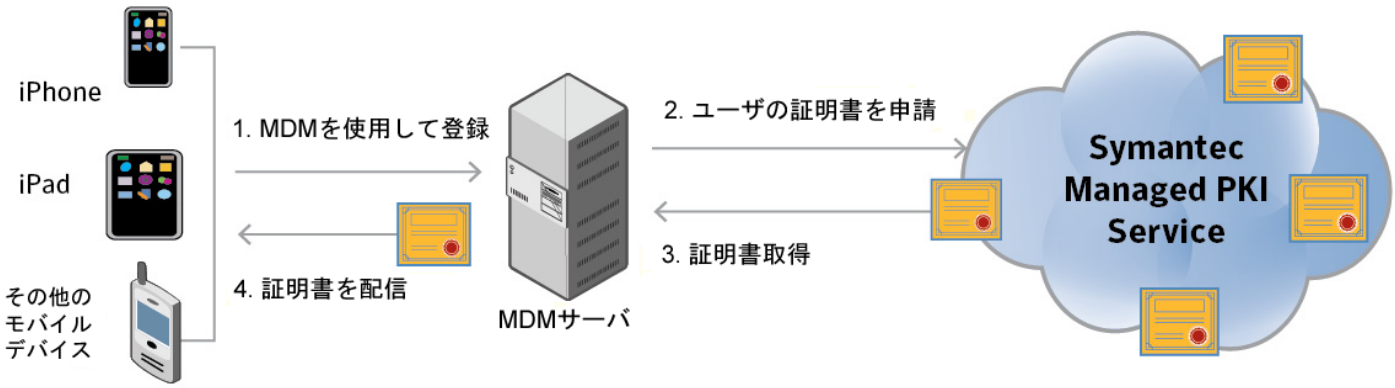

図3：MDMシステムとの併用

MDMソリューションとSymantec Managed PKI Serviceの統合は、Symantec Managed PKI Serviceのウェブサービスインターフェイスから容易に行えます。（Symantec Mobile Managementソリューションのほか、多くのMDMソリューションをこの方法で統合できます。）MDMからのプロファイルダウンロードを保護には、デバイスID証明書を発行するために使用されるSymantec Managed PKI Serviceから出されるSimple Certificate Enrollment Protocol（SCEP）が利用されます。

直接デバイスからオペレーションを行うモデル

このモデルは、シンプルにモバイルデバイスにMDMと証明書を導入し、他のアプリケーションにも証明書を適用したいと考えている企業に適しています。またこのモデルは、モバイル以外のユーザも同時にサポートする場合に重要です。

デバイスが証明書を直接サポートしていますので、エンドユーザはデスクトップの申請と同様の方法で、モバイルデバイスの証明書を申請できます。その際、申請ページはモバイルデバイス用のフォーマットが用意されています。また、証明書のインストールと証明書を使用するアプリケーションの双方を自動的に構成しますので、ユーザとIT管理者の負担を軽減できます。

たとえばApple iOSでは、Symantec Managed PKI Serviceは組み込みのiOS OTAプロトコル機能を活用して、iOSデバイスやアプリケーションがSCEPを介して証明書の申請を行えるようにします。その後Managed PKI Serviceは、証明書とともにiOS OTA構成プロファイルを配信します。これによりデバイスは、該当するすべてのアプリケーションで証明書を使用するように自動構成を行います。
次の図は、iOSデバイスにおけるこのプロセスを示しています。

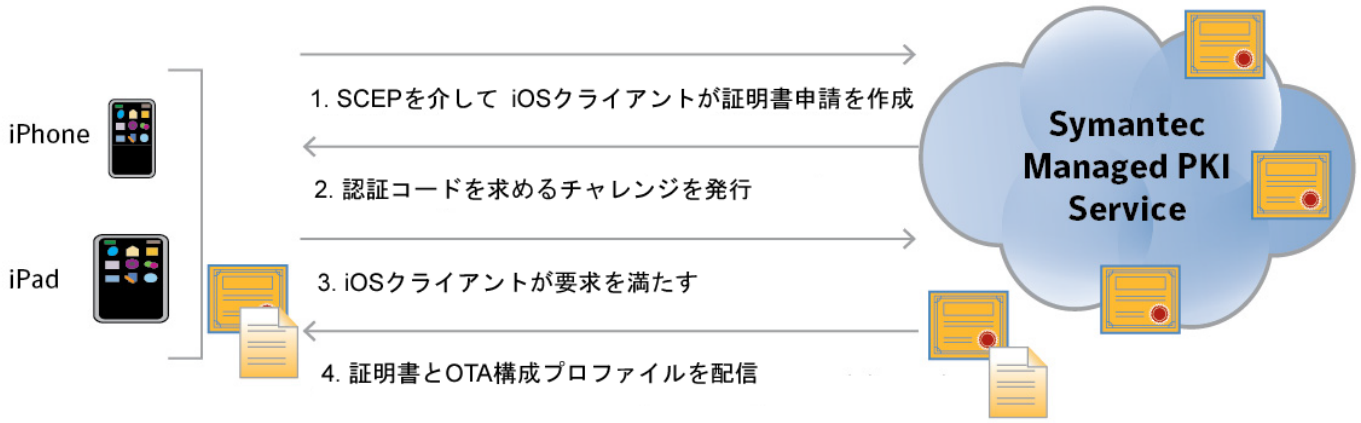

図4：モバイル対応の証明書サービスによるデバイスの直接サポート

iOSでSymantec Managed PKI Serviceを使用する主なメリットは、もう1つあります。サービス管理ワークフローによって、デバイスの証明書形式と申請オプションが定義されるのと同時に、管理者がデバイスのOTA構成管理プロファイルを定義できるため、管理者の作業がはるかにシンプルになるという点です。

Microsoft Windows®タブレットなど、iOS OTAのような機能がないデバイスに関しては、シマンテックではWindows PKI Clientを提供しています。Windows PKI Clientにより、デバイスやアプリケーションで証明書を使用するよう構成する作業がシンプルになります。また、シマンテックは、今後Android向けクライアントの提供も予定しています。

まとめ

電子証明書は、パスワードなど他のクレデンシャル技術とは一線を画し、PKI基盤を利用した認証強化による強固なセキュリティを実現します。また、一度インストールすればパスワードの入力も不要など、とても利便性の高いソリューションです。電子証明書は、業界で主要なセキュリティクレデンシャルであると認められているのみならず、20年にわたる実績で、その有効性が実証されています。さらに、モバイルデバイスの導入でまず考慮するMDMソリューションの安全性を確保するためには電子証明書が必要であるほか、電子証明書をその他の幅広いアプリケーションの保護にもご利用いただけます。

Symantec Managed PKI Serviceは、電子証明書クレデンシャルを用いてモバイルデバイスの認証を強化するリューションです。モバイルデバイスの直接サポートと、Symantec Mobile Management、MobileIron、AirWatch、Fiberlink、Zenprise、CLOMO、MobiConnectなどの主要なMDMパートナーとの幅広い提携関係により、モバイルデバイスのコンテンツセキュリティ管理に優れたソリューションを実現します。
モバイルデバイスは進化を続けており、それに伴い企業の利用シーンも増加傾向にあります。企業はSymantec Managed PKI Serviceが提供するクレデンシャルによりモバイルデバイスの信頼性を確保し、データを保護し、正しいユーザ以外はネットワークにアクセスさせないことが可能になりますので、ビジネスに安全にモバイルデバイスを活用いただけます。

Symantec Managed PKI Serviceについては、https://www.symantec.com/ja/jp/をご覧ください。

用語集

認証局（CA：Certificate Authority）	公開鍵基盤（PKI：Public Key Infrastructure）において、電子証明書を発行、失効、停止する権限がある信頼できる第三者機関。
電子証明書（Digital Certificate）	安全性が高く信頼できる電子署名の形式。電子署名により、検証済みのユーザID、ドキュメントの整合性、タイムスタンプ、署名済み電子ドキュメントの否認防止が得られます。
災害復旧（Disaster Recovery）	自然災害や人災の発生後に、組織にとって不可欠な技術インフラストラクチャを復旧または継続させるための準備に関する、プロセス、ポリシー、手順。
EJBCA（Enterprise Java Bean Certificate Authority）	スウェーデンの営利企業が維持および出資する、無償のPKI認証局ソフトウェアパッケージ。
MDM（Mobile Device Management）	携帯電話事業者、サービスプロバイダ、および企業にわたって導入されるモバイルデバイスの安全性確保、監視、管理、サポートを行うソフトウェア。MDMの機能には、携帯電話、スマートフォン、タブレットPC、モバイルPC、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、および構成のOver-the-Air（OTA）での配信が含まれます。
OTA（Over-the-Air）	新しいソフトウェアアップデートや構成設定を、携帯電話のようなデバイスに配布するためのさまざまな方式。新しいアップデートやサービスの提供が始まると、OTA構成の重要性が高まります。
公開鍵基盤（PKI：Public Key Infrastructure）	電子証明書の作成、管理、配布、使用、保存、失効に必要な一連のハードウェア、ソフトウェア、スタッフ、ポリシーおよび手順のすべてを説明する包括的な用語。
SCEP（Simple Certificate Enrollment Protocol）	幅広く利用され、多くのテストを経ている、最も一般的な証明書申請プロトコル。電子証明書の発行と失効を、最大限に拡張できるよう設計されています。

シマンテックについて

シマンテックは、セキュリティ、ストレージ、システム管理に関するソリューションのグローバルリーダーとして、あらゆる規模の企業と個人のお客様の情報セキュリティ確保と管理を支援します。米国カリフォルニア州マウンテンビューに本社を置き、世界40か国以上で事業を展開しています。詳細については、www.symantec.comをご覧ください。