DigiCert PKI Platform
サービス記述書

サービスの概要

DigiCert PKI Platform (「PKI Platform」または 「Platform」)は、新しい証明書の発行から、既存の証明書の更新、信頼に値しない証明書の失効まで、証明書のライフサイクル全体を管理するための柔軟なPKI Platformを提供します。また、DigiCert PKI Platformは、電子メール、ファイルシステム、またはその他のデータの暗号化に使用する証明書の秘密鍵の預託や復元もできます。さらに、証明書の現在のステータスを確認するためのさまざまな検証サービスが用意されているので、信頼に値する証明書のみをデータの暗号化、文書へのデジタル署名、ネットワーク接続のための認証などに使用できます。

本サービス記述書は付属の添付書類とともに、DigiCertが提供する本サービス記述書記載のサービスについて、参照により本サービス記述書を組み込んだ契約の一部です (以下総称して「契約書」という)。

目次

技術的/業務上の機能と特性

サービスの機能

DigiCert PKI Platformはマネージドサービスであるため、PKIを社内で構築する場合と比べてコストを大幅に削減できます。例えば、PKIを社内運用して証明書を発行するには、まず、暗号化とアプリケーション用のサーバーハードウェアを調達し、サーバーとクライアントのライセンスを購入して、スタッフを教育する必要があります。さらに、PKI階層の管理に関する基本方針をまとめた証明書ポリシー（CP）や、証明書に関するプロセスと手続きおよび役割と責任を定義した認証局運用規定（CPS）を独自に作成する必要もあります。DigiCert PKI Platformは、暗号化とアプリケーションの運用に最適なサーバーハードウェアを基盤とした可用性の高いマルチテナント環境を提供します。また、この環境は専門教育を受けたうえで厳格な身元調査に合格したスタッフが24時間365日監視しています。さらに、WebTrustとSAS70の認定を維持するために監査を定期的に受けています。

- DigiCert PKI Platformでは、**認証局（CA）**階層を構築および管理できます。
  - DigiCert PKI Platformは、以下の標準認証局階層で利用できます。
    - DigiCert Trust Network – ***付録Aを参照***
    - プライベート認証局 – ***付録Bを参照***
    - Adobe® ドキュメント認証サービス – ***付録Cを参照***
    - LTE Certificate Service – ***付録Dを参照***
    - 製造元発行の証明書 – ***付録Eを参照***
  - 各サービスアカウントには、選択した認証局階層ごとに少なくとも1つの認証局証明書が含まれています。特定のボリュームの追加の認証局証明書は、後ほど購入できます。DigiCertシステムおよびサービスからの認証局証明書および/または対応する鍵のペアの抽出には、当事者の同意が必要となります。
- DigiCert PKI Platformでは、クラウドとハイブリットの2種類の導入モデルで**証明書ライフサイクルを管理**できます。
  - クラウド導入モデルでは、アカウント、証明書、鍵の管理ツールをDigiCertのデータセンターでホストします。
  - ハイブリッド導入モデルでもアカウント、証明書、鍵管理ツールはすべてDigiCertのデータセンターでホストしますが、登録局（RA）とディレクトリ統合ツールはお客様のデータセンターに配置します。
  - 導入モデルはどちらか一方に統一する必要はなく、さまざまなPKIプロジェクトの必要性に応じて組み合わせて使用できます。どちらの導入モデルでも、デスクトップミドルウェアであるPKI Clientを使用して、証明書ライフサイクルに関するユーザーの操作性を大幅に向上できます。

- DigiCert PKI Platformの提供する管理ツールは次の通りです。
  - **PKI Manager** – PKI ManagerはDigiCertデータセンターでホストされる、PKI管理者向けのWebポータルです。このツールを使って、アカウント、ユーザー、証明書、鍵管理に関するタスクを実行できます。
    - アカウント管理: PKI管理者は、PKI Managerを使ってアカウントに関連付けられた認証局（CA）、シート数、レポートを確認できます。また、PKI管理者が他のPKI管理者を追加して権限を割り当てることもできます。
    - ユーザー管理: PKI Managerを使ってPKI管理者は、ユーザーを追加したり、各ユーザーに一意のパスコードを生成したり、ユーザーに送信する電子メールをカスタマイズしたりできます。また、新しく発行された証明書をサードパーティアプリケーションで使用するための設定手順を文書やビデオでユーザーに知らせることもできます。
    - 証明書管理: PKI管理者は、PKI Managerを使ってアカウント内の各CAの証明書プロファイルを設定できます。証明書のプロファイルとして、鍵長、鍵の使用法、署名アルゴリズムなどのパラメータを設定できます。また、ユーザーの操作（OS/ブラウザまたはPKIクライアントを通じての登録）およびセキュリティ保護レベルも選択できます。さらに、証明書の秘密鍵を預託するかどうかの選択も可能です。証明書プロファイルの設定に加えて、ユーザーが退職するなどして不要になった証明書や、ノートPCの紛失によって秘密鍵が危険に晒されたなどの理由で信頼に値しない証明書を失効させることもできます。
    - 鍵管理: PKI Managerを使ってPKI管理者は、暗号化用の証明書の秘密鍵を復元できます。
  - **PKI証明書サービス** – PKI証明書サービスは、DigiCertのデータセンターでホストされるサービスで、ユーザー（利用者）が証明書を要求する証明書登録Webページを提供します。これらのWebページは、証明書を要求するのに必要な手順をユーザーに案内します。PKI管理者は、このWebページにサードパーティ製品の設定手順を表示することもできます。
  - **Certificate Issuance Center** – Certificate Issuance CenterはDigiCertデータセンターでホストされる証明書エンジンです。この証明書エンジンでは、PKI Certificate Service、PKI Enterprise Gateway、またはWebサービスから送られたCSRを利用して証明書が作成されます。また、発行元認証局（CA）による証明書への署名もここで行われます。
  - **PKI Enterprise Gateway** – PKI Enterprise Gatewayは、必要に応じてお客様のデータセンターにインストールされる登録局（RA）アプリケーションです。Lightweight Directory Access Protocol (LDAP)ソース(例えばMicrosoft® Active Directory®)と密接に連携して、証明書要求の承認やLDAPソースへ の証明書データの追加を自動化します。
  - **PKI Client** – PKI Clientは、証明書ライフサイクルに関するユーザーの操作性を大幅に向上させることを目的としたエンドポイントミドルウェアです。PKI Clientは、WindowsオペレーティングシステムとMacオペレーティングシステムのデスクトップで利用できます。ユーザーは、Microsoft Internet Explorer®、Safari®、Chrome™またはMozilla® Firefox®を使用して、証明書の登録Webページから証明書を要求します。ネイティブで操作する場合、追加のソフトウェアは不要ですが、一般的に操作性は低下します。例えば、Microsoft Internet Explorerでは、警告メッセージを表示するポップアップウィンドウが多数表示されて、ユーザーを煩わせることがあります。PKI Clientを使用すれば、よく使われる機能（証明書の更新など）を自動化することでユーザーの操作を最小限に抑え、証明書ライフサイクルの管理を効率化できます。また、集中型のポリシー管理機能（PINやエクスポートなど）も提供されるため、証明書の保護にも役立ちます。さらに、証明書を使用するようにサードパーティ製品（ワイヤレスネットワーククライアントや仮想プライベートネットワーククライアントなど）を自動設定することも可能です。DigiCert PKI Platformの証明書ライフサイクル管理機能は、モバイルデバイスからも利用できます。iOSの場合は、内蔵のOTA（Over-the-Airプロトコル機能が利用されます。このため、iOSデバイスやiOSアプリケーションでは、Apple社のSCEPプロトコルを介して証明書登録を要求できます。iOSのOTAに相当する機能を持たないAndroid OSなどのモバイルオペレーティングシステムでは、DigiCertが提供する専用のPKI Clientを使って、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簡単に設定できます。

- **PKI Webサービス** – PKI WebサービスはDigiCertデータセンターでホストされるサービスで、DigiCert PKI Platformとプログラム的に統合する機能を提供します。サードパーティ製アプリケーションは、PKI Webサービスで提供されるAPIを使って、証明書ポリシーを取得したり、証明書ライフサイクル機能（登録や更新など）を実行したりできます。

- DigiCert PKI Platformで利用可能な**認証方法は次の通りです。**
  - **申請コードを使用した認証** – このタイプの認証では、PKI 管理者が各ユーザー用に、証明書要求を自動的に承認するための一意の申請コードを生成します。PKI 管理者は、証明書登録Webページへのリンクを記載した証明書案内メールをユーザーに送信する際に、そのユーザー用の一意のパスコードを一緒に記載します。ユーザーは、証明書登録Webページで、他の情報とともに自分のパスコードを入力します。Certificate Issuance Centerでは、ユーザーが入力した申請コードと、PKI Managerで生成された情報が照合されます。一致した場合は、Certificate Issuance Centerから証明書が発行されます。一致しない場合は、ユーザーにエラーメッセージが表示されます。
  - **自動認証** – 自動認証では、LDAPデータソース（Microsoft Active Directory など）のデータに基づいて証明書要求が承認されます。この認証方法を使用するには、お客様のデータセンターにPKI Enterprise Gateway をインストールして、LDAP ソースと連携させる必要があります。ユーザーがPKI Certificate Serviceを介して証明書要求を送信すると、PKI Enterprise Gatewayで証明書要求のデータとLDAPソースのデータが照合されます。データが一致すると、PKI Enterprise Gatewayは証明書の要求を承認し、登録局（RA）証明書によって署名され、署名された証明書要求がCertificate Issuance Centerに送信されます。一致しない場合は、証明書要求が却下されます。

- DigiCert PKI Platformで利用可能な**証明書検証ツールは以下の通りです。**
  - **証明書失効リスト(CRL)** – 多サードパーティ製品の多くは、証明書失効リスト（CRL）を使って証明書の現在のステータス（有効や失効など）を確認する機能を備えています。CRLは、有効期限切れになる前に失効した証明書が記載される一種のブラックリストです。これらの製品では、最新のCRLを定期的にダウンロードしてステータスを確認するように設定できます。証明書がCRLに記載されている場合はアクセスが拒否されます（ネットワーク認証に失敗する、文書にデジタル署名できないなど）。DigiCertでは、少なくとも24時間に1回の間隔でCRLを生成してします。
  - **オンライン証明書ステータスプロトコル (OCSP)** – サードパーティ製品の多くは、オンライン証明書ステータスプロトコル (OCSP) を使用して証明書の現在のステータス（有効や失効など）を確認する機能も備えています。失効した証明書はすべてのCRLに記載されますが、証明書が失効してから新しいCRLが生成されるまでには、標準のCRLで最大24時間の遅延が生じます。DigiCertのOCSPツールTGV（Trusted Global Validation）では、証明書のステータス変更（失効や停止など）があったときに、ほぼリアルタイムで変更が反映されます。

- DigiCertは、DigiCert PKI Platformを補完するために以下の**ハードウェアオプション**を提供しています。
  - **SafeNet® PKIトークン** – DigiCertはSafeNet® ハードウェアUSBトークンの認定リセラーです。さらに、これらのトークンはリポジトリに収録されている保証情報の補足に記述されているように年間の保証が付きます。これらのトークンは、FIPS（連邦情報処理規格）140-2およびCC（Common Criteria）標準に準拠しています。
  - **SafeNet® ハードウェアセキュリティモジュール(HSM)** – DigiCertは、Luna® PCIカード、Luna® SAネットワークアプライアンス、Luna® PCMトークンで構成されるSafeNet® Luna® ハードウェアセキュリティモジュール(HSM)の認定リセラーです。これらのHSMには、ファームウェアまたは関連ソフトウェア(SafeNet Authentication Clientなど)が含まれることもあります。HSMには1年間の基本保証が付いていますが、DigiCertはSafeNet延長保証プログラムをオプションとして有償で提供しています。これらのHSMもFIPS 140-2レベル2およびCC標準に準拠しています。
    - 販売されたあらゆるHSMの所有権は、DigiCertから出荷時にお客様またはお客様が指名した当事者に譲渡されます。すべての製品はDigiCertの出荷地点における工場渡し（EXW）- インコタームズ 2010 - となります。HSMの製品引き渡しはDigiCertの出荷地点で運送会社に該当製品が渡った時に完了します。運賃条件は、着払いまたは第三者支払いでなければなりません。
    - お客様がDigiCertを通じたHSMの購入を選択し（「お客様のHSM」）そのHSMがDigiCertのデータセンターに保管される場合、お客様のHSMはDigiCert所有のHSMと同じ方法の保護のもと保管されされます。お客様に提供されるDigiCertの該当サービスが満了または終了する際に、DigiCertはお客様の要求に応じて、業界のベストプラクティスに従ってお客様のHSMをお客様に譲渡します。お客様のHSMの譲渡は無償で行われますが、お客様のHSMの譲渡に関してお客様がテクニカルサポートを要請した場合、DigiCertは両当事者が相互に合意する別途交渉の作業記述書の下で譲渡への支援を提供します。
- DigiCertは、DigiCert PKI Platformを通じて、次のタイプの**証明書**または**シート**を提供します。
  - **ユーザーシート:** VPN/WiFiを介してプライベートネットワークにアクセスするユーザーとして認証する利用者（サブスクライバー）に発行される証明書。そのような ***「ユーザーシート」***の下に発行される証明書は、これらのユーザーに複数の異なるタイプのユーザー証明書 (***ユーザーシート***プールからのVPN、WiFi、S/MIMEなど) をこれらのユーザーに発行することを許可します。1つのユーザーシートが、単一で固有のユーザーに発行される複数の証明書を指すことがあります。
  - **デバイスシート:** デバイスがプライベートネットワークにアクセスできるようにするために、デバイス (ノートPC、コンピュータ、LTE機器など) に発行される証明書。ユーザーシートと違って***デバイスシート***はデバイスに発行された証明書であり、1台の物理デバイスのみで使用できます。
  - **サーバーシート:** サーバー上でホストされているイントラネットのWebサイトへのアクセスを要求しているユーザーまたはデバイスに対して、そのサーバーの識別情報を保証するために、利用者（サブスクライバー）として組織の内部サーバーに発行された証明書。DigiCert PKI Platformは、このソリューションの一環としてプライベート階層サーバーの証明書を発行します。各物理サーバーまたは仮想サーバーは、サーバーシートを必要とします。

- **組織証明書:** ID 認証（プライベートコードサイニングの証明書の場合など）およびデジタル書名（組織レベルでのWordまたはPDF署名の場合など）を許可するために、サブスクライバーとしての組織または団体に発行される証明書。以下に***組織証明書***の制限について説明します。お客様は、次の場合においてコードサイニングまたは他のいずれの***組織証明書も使用してはなりません:*** (i) お客様の組織以外の組織のために、またはその代理として使用すること。（ii）提出した証明書申請書に記載されているお客様以外のドメイン名および/または組織名に関連して秘密鍵または公開鍵の操作を行うこと。(iii) そのようなコンテンツの受領者に迷惑をかけるような影響を与えるコンテンツを含む（がこれに限定されない）あらゆる種類の悪意のあるコンテンツまたは有害なコンテンツを配布すること。(iv) 証明書の公開鍵に対応する秘密鍵へのアクセスを、お客様が許可した従業員以外の者に委譲する方法で行うこと（そのような譲渡は秘密鍵を保護するために安全な方法で行われるものとする）。

DIGICERTの義務

- 必要な導入作業の完了後、DigiCertは本サービス記述書に明示されているサービスをお客様に提供します。
- DigiCertは、お客様とお客様側のPKI Platform管理者からの指示に従って、証明書を発行、管理、失効、および/または更新を行います。
- お客様の証明書申請の承認時にDigiCertは: (1) そのような承認された各証明書申請書の情報の正確性に依拠する権利を有します。(2）当該の証明書申請書が送信された証明書申請者に対し証明書を発行します。
- 管理者証明書を含む本サービス記述書のもとで発行またはライセンスを授与された証明書は、各証明書が発行された日から最高12ヶ月間有効です。
- 単一の認証局の鍵生成イベント中に、DigiCertはDigiCert Trust Networkまたはお客様が選択する他の階層で、お客様に代わってDigiCertにより発行された証明書の署名に使用する、お客様用の認証局鍵のペアを生成します。
- 各鍵ペアのお客様の認証局秘密鍵は、1つ以上のハードウェアセキュリティモジュールに保存されます。

お客様の責任

DigiCertは、お客様が必要な情報を提供した場合または必要な操作を実行した場合のみ、サービスを提供することができます。お客様が次の義務を提供/履行しない場合、以下に記載するようにDigiCertによるサービスの実行に遅延、障害または阻害が生じることがあります。

- セットアップの有効化: お客様にDigiCertがサービスの提供開始に必要とする情報の提供をお願いする場合があります。
- 適切な担当者: お客様はDigiCertから合理的な要望に応じて、DigiCertがサービスを行うために適切な支援をする人材のアサインをお願いすることがあります
- お客様は以下を確保する必要があります:
  - 証明書発行のためのすべての情報資料は、すべての重要な点において真実であり、正しいこと。
  - お客様による証明書申請の承認により誤った証明書を発行しないこと。

- お客様の証明書の失効が、DigiCert Trust Network CPSまたはAdobe CPSに準拠すること (該当する場合)。
- お客様が、DigiCert Trust Network CPSまたはAdobe CPSを十分に遵守すること (該当する場合)。
- お客様は登録局の要件に十分に準拠していること (該当する場合)。
- DigiCertに提供された証明書情報が第三者の知的財産権を侵害しないこと (ドメインスクワッティングなど)。
- 証明書申請書の情報 (電子メールアドレスを含む) が違法な目的のために使用されておらず、今後も使用されないこと。
  - お客様側のPKI Platform管理者は、(管理者証明書の作成時以降)将来にわたり 管理者証明書の秘密鍵を保持し、秘密鍵を保護するチャレンジフレーズ、PIN、ソフトウェア、または秘密鍵を保護するハードウェアメカニズム扱うことができる唯一の人物となります。許可されていない者はそのような資料や情報にアクセスすることがなく、今後もアクセスすることができません。
  - お客様は、このサービス記述書に遵守し、許可された合法的な目的のためにのみ管理者証明書をご使用いただきます。
  - お客様は、DigiCertシステムまたはソフトウェアの技術的な実装を監視、干渉またはリバースエンジニアリングしたり、DigiCertシステムまたはソフトウェアのセキュリティを故意に侵害することはできません。

支援とテクニカルサポート

DigiCertのサポートとメンテナンスのコミットメントは、リポジトリに収録されているサービルレベル契約に記述されています。

サービス固有の条件

自動更新なし

本契約書のいかなる規定にもかかわらず、NSLサービスの自動更新はありません。NSLサービスの有効期限が切れる前にお客様はDigiCertまたはDigiCertのチャネルリセラーパートナーにご連絡ください。

サービス条件

- **管理者証明書:** お客様が管理者証明書の証明書申請を送信し、DigiCertが管理者証明書に必要な認証手続きを完了した後で、DigiCertはその証明書申請を処理します。DigiCertは、お客様の管理者証明書の申請が承認または却下されたことをお客様に通知します。PKI Platform管理者がDigiCertから受領したPINを使用して管理者証明書を取得するか、または管理者証明書をインストールまたは使用すると、PKI Platform管理者が管理者証明書を受け入れたこととなります。PKI Platform管理者が管理者証明書を取得またはインストールした後、PKI Platform管理者は、その証明書を使用する前にその情報を確認し、誤りがあった場合には迅速にDigiCertにご連絡ください。そのような通知の受領後、DigiCertはその管理者証明書を失効し、修正した管理者証明書を発行することが可能となります。
- **存続:** 本契約書に記載されている終了条項に加えて、本サービス記述書および該当するいかなるCPSの失効およびセキュリティ要件は、本契約書または該当する注文書の終了後も、本契約に基づいて発行されたすべての証明書の運用期間が終了するまで存続します。

- **現地法の遵守:** お客様は、DigiCertが本サービス記述書に従って生成した公開鍵と秘密鍵のペアの取得、使用、または受諾が、輸出入に関する法律、規則、規制などを含むがこれらに限定されない、現地の適用法、規則および規制に確実に従う責任があります。
- **監査権限:** DigiCertは、本サービス記述書の条件への遵守を確実にするために、1年に1回お客様の手順を監査することがあります。このような監査は、妥当な書面による通知を受けてから営業時間内に実施され、お客様の業務活動を不当に妨害することはありません。お客様は、このような監査すべてに関し、必要と判断される範囲に関しDigiCertに協力ください。監査によって、お客様が本サービス記述書の利用規約に違反していることが明らかになった場合: (1) お客様は、監査の実施にかかる相応の費用がDigiCertへの支払いとして生じます。その上、(2) 上記の1年に一度の監査にかかわらず、DigiCertは本書の利用規約への遵守を徹底するための追加監査を合理的に必要と思われる範囲で実施することがあります。年1回の定期監査は、前年の活動のみを対象とすることができます。
- **使用の制限:** サブスクライバーに発行された証明書は、該当する証明書要請に対応しない証明書利用者は実装またはインストールできない場合があります。各証明書は、証明書のタイプが示すとおり、意図された使用のためにのみ使用されなければなりません。
- 以下に示すように、認証局階層に固有の追加条件を参照してください:
  - DigiCert Trust Network – ***付録Aを参照***
  - プライベート認証局 – ***付録Bを参照***
  - Adobe®ドキュメントサイニングサービス – ***付録Cを参照***
  - LTE証明書サービス – ***付録Dを参照***
  - 製造元証明書 – ***付録Eを参照***
- ソフトウェア形式のあらゆるサービスコンポーネントの使用には、ソフトウェアに付属の使用許諾契約が適用されます。サービスコンポーネントにエンドユーザー使用許諾契約書が付随していない場合は、リポジトリに収録されている「b-hosted-service-component-eula-eng.pdf」の利用規約に準拠するものとします。当該のサービスコンポーネントの使用に関する追加の権利および義務は、本サービス記述書に記載されているとおりとします。
- 本サービス記述書に特に明記されていない限り、本サービス (本サービスで提供されているホスト型サービスソフトウェアコンポーネントを含む) には、別途ライセンスの対象となるオープンソースおよび他の第三者のマテリアルが使用されることがあります。該当する場合は、以下で当該サードパーティの通知を参照してください: https://www.websecurity.symantec.com/legal/repository#managed-pki-service

- DigiCertは、本サービスの有効性を維持するために、いつでも本サービスを更新することができます。
- 本サービスは、適用される輸出規制の制限及びその当時の技術的な制限に従って、世界中でアクセスして使用できます。

評価用ライセンス

本条の条件は、お客様が評価目的で本サービスにアクセスしている場合に適用されます。

- **使用権。**お客様に付与されたライセンスは、実稼働環境でないテスト環境において、本サービスを社内で非商業的に評価し、互換性をテストする目的での使用に制限されます。お客様は、その他いかなる目的でも本サービスを使用することはできません。
- **評価期間。**お客様に供与されるライセンスは期間が制限されており、お客様の評価用ライセンスの登録時に指定された試用終了日まで有効となります（「評価期間」）。お客様が本サービスの商用ライセンスを購入しない限り、お客様に供与されたライセンスは評価期間の満了時に終了します。
- **終了後。**ライセンス終了時にお客様は、本サービスの使用を中止する必要があります。終了によって、終了日より前に発生した義務はいずれの当事者からも免除されることはありません。終了、取消または満了の後も存続することが本質的に意図された条件は存続します。
- **責任の制限。**いかなる場合も、DIGICERTは、収益の損失、利益の損失、または結果的損害を含むがこれらに限定されないいかなる損害についても、たとえその可能性が知らされていた場合でも、一切責任を負いません。
- **免責事項。**本サービスにDIGICERTが一般の利用可能性を公表していない技術が含まれる場合、本サービスは、一般的に利用可能な製品のレベルで実行できないことがあります。本サービスは正しく動作しない可能性があり、最初の商用リリースがある場合は、その前実質的に変更されることがあります。両当事者は、合意の上で評価目的のためにお客様に提供される本サービスまたはソフトウェアは、「現状のまま」提供されるものであり、一切の保証が適用されないことを認めるものとします。DIGICERTは、商品性、特定目的への適合性、第三者の権利の非侵害における暗黙の保証を含むがこれらに限定されない、あらゆる明示的、黙示的または法的な保証に対して責任を負わないものとします。両当事者はまた、本サービス記述書は本サービスを説明する目的でのみ存在し、サービス記述書に含まれるすべてのDIGICERTの表明、保証、サービスレベルの確約、義務または責任は、本契約の基づきDigiCertによって放棄されることを認めるものとします。DIGICERTのいかなる代理人または雇用者にも、本保証の変更、延長または追加する権限はありません。
- **優先順位。**この条項と本契約の別の条項との間に抵触が生じた場合、本サービスが評価目的で提供されている限り、本条項が優先されます。

MICROSOFT自動登録コンポーネントの使用

お客様がPKI PlatformのMicrosoft自動登録コンポーネントを使用する場合は、以下のMicrosoftサポート補足義務が適用されます:

(a) **免責。**Microsoft 社とその関連会社は、この取り決めに従って提供されるサーバーソフトウェア（「サーバーソフトウェア」）について一切の明示的、黙示的、法的保証をせず、その実行または実行不能について一切の責任を負いません。Microsoft 社のサーバーソフトウェアは、何ら保証のない現状有姿のままで提供されます。Microsoft 社とその関連会社は、本文書によって、サーバーソフトウェアに関するその他一切の明示的、黙示的、法的な保証、義務、条件（商品性、特定目的への適合性、信頼性、可用性に関する黙示的な保証と条件を含むが、これに限定されない）を免責されるものとします。また、Microsoft 社とその関連会社は、サーバーソフトウェアに関して、権原、平穏享有、説明との一致、非侵害性に対する一切の保証および条件を免責されるものとします。

(b) **特定の損害の除外。**適用される法律によって許容される最大限の範囲で、いかなる場合においても、Microsoft 社は、サーバーソフトウェアの使用または使用不能、あるいはサーバーソフトウェアを通じたサポートやその他のサービス、情報、ソフトウェア、関連コンテンツの提供または不提供、あるいは本サービス記述書の条件に起因もしくは関連する、特別損害、付随的損害、懲罰的損害、間接損害、結果的損害、その他一切の損害（利益の損失、機密情報やその他の情報の喪失、事業の中断、人身傷害、プライバシーの喪失、誠実義務の不履行、注意義務の不履行、過失、その他の金銭的損失、その他一切の損失による損害を含むが、これに限定されない）に対して、それが Microsoft 社の過失、不法行為（怠慢を含む）、厳格責任違反、契約違反、保証違反によるものであったとしても、また、かかる損害が発生する可能性をMicrosoft 社が事前に通知されていた場合であっても、一切の責任を負わないものとします。

(c) **サーバーソフトウェア要件。**サーバーソフトウェア要件 お客様は、この取り決めに従って提供されるサーバーソフトウェアを、ネーティブの Microsoft Windows 2000 Professional 、Windows XP Home/Professional、Windows Vista、またはその後継となるクライアントオペレーティングシステムとの相互運用や通信のみを目的として、本ソフトウェアの付属文書に明示されているとおり 1部のみ使用できます（適用されるサービス注文書または作業範囲記述書で別途明示されている場合を除く）。お客様は、いかなる状況であっても、パーソナルコンピュータ上でサーバーソフトウェアを使用することはできません。前記において**「パーソナルコンピュータ」**とは、一度に 1 人のユーザーが使用することを主な目的として構成され、ディスプレイやキーボードを備えたコンピュータを指します。

(d) **第三受益者。**契約の条項と矛盾する場合でも、本文書によってお客様は、Microsoft社が、サーバーソフトウェアに含まれる知的財産権のライセンサーとして本サービス記述書の条件における第三受益者となり、かかる Microsoft 社の知的財産や本条件に関連するMicrosoft 社のその他の権益に影響を与える本条件の条項を行使する権利を持つことに同意するものとします。

(e) **サーバークラス2。**お客様がサーバークラス 2を選択した場合、お客様は、（a）処理能力が最大 32 ビットで RAM が最大 4 GB のプロセッサ 4 基以下で構成され、（b）サーバーを再起動せずにメモリの追加、交換、取りはずしができる能力（「**ホットスワップ機能**」）を持たないサーバー上で、サーバーソフトウェアを使用できます。**ホットスワップ機能**やクラスタ機能をサポートするソフトウェアをサーバーソフトウェアと組み合わせて使用することはできません。「クラスタ機能」とは、複数のサーバーをグループ化し、グループ内のサーバーノード間でのアプリケーションフェールオーバーを実装することによって、アプリケーション実行のための単一の高可用性プラットフォームとして機能させることを指します。

(f) **監査権**。DigiCertは、お客様が本条件のすべての条項に準拠していることを確認するため、監査を実施し、通常の営業時間中にお客様の敷地内でお客様の施設と手続きを調査する場合があります。監査の際には、少なくとも 14 日前までにお客様にその旨を通知します。契約の条項と矛盾する場合でも（機密保持規定を含むが、これに限定されない）、お客様が監査の実施を拒否し、お客様がサービス記述書の条件に準拠していないとDigiCertが判断する十分な理由がある場合には、DigiCertがお客様の身元情報とお客様が不適合であると考える根拠を Microsoft 社に開示することにお客様は同意するものとします。

(g) **多重化デバイス**。サーバーソフトウェアで提供されるサービスに直接接続するユーザーやそれらを直接使用するユーザーの数を減らすハードウェアまたはソフトウェアを使用した場合でも、接続ユーザーまたは使用ユーザーと見なされるユーザーの数は減りません。サーバーソフトウェアの接続ユーザー数または使用ユーザー数は、直接であるか多重化デバイスを介するかに関係なく、（a）サーバーソフトウェアまたは（b）サーバーソフトウェアが認証を行うその他のソフトウェアやシステム（「**その他の認証対象システム**」）によって提供されるサービスに接続するユーザーまたはそれらを使用するユーザーの数と等しくなります。ここで述べる「**多重化デバイス**」とは、サーバーソフトウェアまたはその他の認証対象システムによって提供されるサービスに直接的または間接的に、あるいは複数のユーザーが少ない接続数でアクセスできるようにするためのハードウェアまたはソフトウェアを指します。

(h) **Windows CAL要件**。お客様は、直接であるか多重化デバイスを介するかに関係なく、サーバーソフトウェアまたはその他の認証対象システムによって提供されるサービスに接続する各ユーザーまたはそれらを使用する各ユーザーに、個別の Windows CAL を取得して割り当てる必要があります。「**Windows CAL**」とは、（a）Microsoft Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition またはその後継となるサーバーオペレーティングシステム製品（「**Windows Server**」）の Windows Device クライアントアクセスライセンス（「**CAL**」）または Windows User CAL、（b）Windows Server にアクセスして使用する権利を個々のユーザーや電子デバイスに与える Microsoft Core CAL を指します。この（a）と（b）のいずれの場合でも、CAL は、1 つ以上の Microsoft Windows Server オペレーティングシステム製品または電子デバイスで使用するために取得し、ユーザー単位またはデバイス単位で割り当てます。

サービスレベル契約。

サービスの可用性におけるDigiCertの誓約は、リポジトリに収録されているサービルレベル契約に記述されています。

定義

本サービス記述書で大文字で記載され、契約書または本サービス記述書に別途定義されていない用語は、以下に示す意味を持ちます:

「管理者証明書」とは、PK Platform管理者として任命されたお客様側の従業員またはその他の信頼される者に対し、PKI Manager にアクセスして管理業務を行うことのみを目的としてDigiCertが発行する証明書を意味します。

[付録D – LTE証明書サービスのみ]「管理者証明書」とは、お客様が任命したサービス管理者、またはPKI Platform管理者として任命されたその他の信頼される者に対し、Webポータルにアクセスして LTEエンドエンティティのデバイス証明書を管理することを目的としてDigiCertが発行するクライアント証明書を指します。

「関連する個人」とは、お客様と関係のある人物を指します。(1) 役員、取締役、従業員、パートナー社員、契約社員、インターン、その他お客様の組織内の人物、または (2) お客様の組織と契約関係を結び、身元を確実に保証できるビジネス記録をお客様が所有している人物が該当します。

「認証局証明書」とは、認証局に発行されたデジタル証明書を意味します。

「証明書」または**「デジタル証明書」**とは、最低限、発行元の認証局の名前または識別情報、利用者、利用者の公開鍵、証明書の運用期間、証明書のシリアル番号、および発行元の認証局のデジタル署名を含むデジタル記録を意味します。

「証明書の申請者」とは、認証局による証明書の発行を要請する個人または組織を意味します。

「証明書の申請」とは、証明書の発行を証明書の申請者 (または許可された代理人) から認証局への証明書の発行の要請を意味します。

「認証局」または**「CA」**とは、証明書の発行、停止または失効する権限を持つ個人またはエンティティを意味します。

「証明書管理プロトコル」または「CMP」とは、LTE証明書または製造元証明書の自動登録とライフサイクル管理のためのプロトコルを意味します。デバイスはCMPを介してDigiCert PKI Platformと直接通信します。デバイスからCMP要請をDigiCert PKI Platformに送信できるようにするには、PKI Platform管理者が前もってデバイスを認可する必要があります。

「証明書運用規定」または**「CPS」**とは、認証局または登録局がによる証明書発行業務の運用規定を定めた文書を指します。この文書は必要に応じて改訂されます。DigiCert Trust Network CPSおよびAdobe CPSは、DigiCert Webサイトのリポジトリに収録されています。

「お客様」とは、本サービスを使用するエンティティを意味します。

「誤発行」とは、（a）DigiCert Trust Network CPS で定められた手順とは大きく異なる方法で証明書を発行すること、（b）証明書の主体として指定されている人物とは異なる人物に証明書を発行すること、（c）証明書の主体として指定されている人物の認可なく証明書を発行することを指します。

「エンドユーザー使用許諾契約」または**「EULA」**とは、ソフトウエアに付随する利用規約を意味します。

「鍵生成」とは、DigiCertがお客様のCA公開鍵/秘密鍵を厳密な手順に従って適切に生成し、生成された秘密鍵と関連ドキュメントを保管する手続きを指します。

「LTE証明書」とは、名前、発行元の認証局または通信事業者ネットワーク内のネットワーク構成要素を含む、デバイスに保存されるメッセージを意味します。ネットワーク構成要素には、通信事業者の基地局、セキュリティゲートウェイ、その他同様のデバイスが該当します。いずれの場合でも、LTE 証明書には、ネットワーク構成要素の公開鍵、証明書有効期間、証明書のシリアル番号、発行元認証局のデジタル署名が含まれます。

「PKI Platform管理者」とは、登録局の従業員、または登録局の業務を行う権限を与えられたその他の信頼される者を指します。

[付録D – LTE証明書サービスのみ]「PKI Platform管理者」とは、本サービス記述書に記載されている特定の証明書関連の管理機能を実行するために任命されたお客様または関連会社の信頼できる従業員を意味します。

「製造元」とは、流通および販売のためにデバイスを製造するビジネスエンティティを意味します。

「製造元証明書」とは、製造時にデバイスに発行され、デバイスに埋め込まれ、通常35～40年の長期間存続し、失効メカニズムを必要としない証明書を意味します。

「運用期間」とは、証明書が発行された日時（または証明書に記載されている特定の日時以降）に始まり、証明書の有効期限の満了時、または早期失効となった日時で終わる期間を意味します。

[付録D – LTE証明書サービスのみ]「運用期間」とは、証明書が発行された日時から証明書の有効期限が切れる日時までの期間を意味します。

「通信事業者」とは、通常は他の国または地域に置かれ、DigiCertがお客様のサブアカウントとして扱う、お客様の関連会社である事業体を意味します。

「プライベート階層」とは、DigiCert Trust Network以外の階層で証明書を発行する認証局と、お客様が定めた基準に従って、お客様のルート認証局から1つ以上の認証局を通じてサブスクライバーに至るチェーンで証明書を発行する認証局のシステムで構成されるドメインを意味します。プライベート階層で発行される証明書は、発行を許可する組織のニーズを満たすことを目的とし、公共チャネルを通じての組織や個人間のやりとりを意図していません。

「秘密鍵」とは、デジタル署名の作成に使用される数学的な鍵を指します。この鍵は他人に知られないように、所有者が秘密に保管する必要があります。アルゴリズムによっては、対になる公開鍵で暗号化された機密のメッセージやファイルを復号するためにも使用されます。

「公開鍵」とは、対になる秘密鍵で作成された署名の検証に使用される数学的な鍵を指します。この鍵は一般に公開されます。アルゴリズムによっては、メッセージやファイルを暗号化するためにも使用されます。暗号化されたメッセージやファイルは、対になる秘密鍵で復号できます。

「登録局」または**「RA」**とは、証明書申請者の身元確認と認証、証明書失効要求の手続き開始と伝達、証明書の更新または鍵更新の申請承認を行うエンティティを指します。RAは、証明書申請者の代理人とは異なります。RAは、RAの認可されたPKI Platform管理者以外に証明書申請の承認権限を委任することはできません。

「信頼される者」とは、証明書および/またはデジタル署名を信頼して行動する人、エンティティまたは物体を意味します。信頼される者は、利用者であることも、そうでないこともあります。

「リポジトリ」とは、https://www.websecurity.symantec.com/legal/repository に収録されているドキュメントのコレクションであり、当該の認証局運用規定の遵守の目的により保持されます。

「ルート認証局」とは、信頼される階層のドメインのトップエンティティであり、ルート認証局は「ルート証明書」によって識別されます。

「シート」とは、サービスの正規エンドユーザーである単一の利用者を指します。その利用者に実際に発行された証明書数は関係ありません。

「サービスコンポーネント」とは、本サービスを受けるために、それぞれのお客様のコンピュータにインストールする必要のある、本サービスが必要とするソフトウェアを意味します。サービスコンポーネントには、本サービスの一部としてDigiCertが別途に提供するソフトウェアおよび関連ドキュメントが含まれます。

「ソフトウェア」とは、DigiCertまたはライセンサーのオブジェクトコード形式の各ソフトウェアプログラムであり、DigiCertによってお客様にライセンスが付与され、該当する場合、本契約に基づいて新しいリリースおよび更新版が含まれますがこれらに限定されず、付随するEULAまたは本サービス記述書の利用規約によって管理されます。

「利用者」とは、証明書の主体であり発行対象である個人、エンティティ、または物体を指します。利用者は発行時に証明書に記載されている公開鍵に対応する秘密鍵を使用することができ、使用する権限を持ちます。

「利用規約」とは、証明書に関する利用者の権利と義務を管理する指定された証明書関連サービスの提供に関連して、利用者と認証局またはDigicertとの間で締結される契約です。DigiCert Trust Network利用規約は、DigiCertウェブサイトのリポジトリに収録されています。

「サブスクリプションインスツルメント」とは、本サービスに関連するお客様の権利と義務をさらに規定する以下の該当する文書の1つまたは複数を意味します:　DigiCert証明書またはDigiCertが発行した類似のドキュメント、またはお客様とDigiCertの間で本サービスに付随、先行または続く書面による契約。

「DigiCert Trust Network」とは、DigiCert Trust Network CPS証明書ポリシーの下で管理される、証明書ベースの公開鍵基盤（PIK）を指します。DigiCertおよびその関連会社、それぞれのお客様、利用者、依拠する当事者は、この基盤を利用して証明書をグローバルに展開および使用できます。

「信頼される者」とは、とは、お客様およびお客様の製品、サービス、設備、手順の基盤をなす信頼性に対して責任を持つ、お客様の従業員、契約社員、コンサルタントを指します。

付録。

付録A: DigiCert Trust Network

DigiCert PKI Platformは、DigiCert Trust Network から証明書を発行する機能をお客様に提供します。DigiCertは、ハードウェアベンダーやソフトウェアベンダーの協力の下で、DigiCert Trust Network の主認証局（PCA）を一般的なほとんどの Web ブラウザ、電子メールアプリケーション、オペレーティングシステム、ネットワークアプライアンスに前もって登録しています。そのため、これらのアプリケーションでは、DigiCert Trust NetworkのPCAのいずれかに関連付けられた証明書が自動的に信頼されます。これらの証明書は、通常、管理者やユーザーが特別な準備をしなくても他の組織との間で使用できます。たとえば、多くのお客様が、DigiCert Trust Network 証明書を使用して電子メールにデジタル署名を付けたり、電子メールを暗号化したりしてセキュリティを強化しています。

標準パッケージでは、すべてのお客様が、クラス2のPCAにつながる発行元認証局（CA）を自動的に利用できます。別の商標名を使用したい場合や、CA のデフォルト値を変更したい場合は、追加の CA を作成するオプションを購入することもできます。

注: これらの証明書を発行、管理、使用するには、お客様とユーザーがDigiCert Trust Network認証局運用規定（CPS）に準拠する必要があります。

追加サービス条件 – DigiCert Trust Networkのみに適用

任命。本文書によって、DigiCertはお客様をDigiCert Trust Network内のDigiCert Trust Network CPSに従う非DigiCert CAとして任命し、お客様はこの任命を受け入れるものとします。

DigiCert Trust Network CPS。本サービス記述書の下でDigiCertに委託された業務を除いて、お客様は、DigiCert Trust Network CPS（改正を含む）およびDigiCert Trust Network内のCAやRAに課されるすべての要件を満たし、すべての義務を果たすものとします。DigiCertは、改正の内容を PKI Managerに掲示することによって、お客様が任命した登録局管理者に通知するものとします。

任命。お客様は、認可された1人以上のお客様側の従業員または信頼される者をPKI Platform管理者として任命する必要があります。任命されたPKI Platform管理者は、お客様に代わって追加のPKI Platform管理者を任命する権利を有するものとします。お客様は、この取り決めに従って証明書を受け取るPKI Platform管理者に、適用される利用規約の条項に従わせる義務を持つものとします。

管理業務。お客様は、DigiCert Trust Network CPS（改正を含む）で定められた要件に従うものとします。これには、証明書申請に含まれる情報の検証、検証後の証明書申請の承認または却下、証明書の失効、DigiCert指定のハードウェアとソフトウェアの使用に関する要件が含まれますが、これに限定されません。お客様は、十分な資格と能力を備えた適切な資質を持つ担当者としてこれらの業務を遂行するものとします。お客様は、証明書申請者がお客様の関連する個人である場合にのみ、証明書申請を承認するものとします。お客様が証明書を発行した利用者がお客様の関連する個人でなくなった場合、お客様はすみやかにPKI Managerから当該利用者の証明書の失効を要求するものとします。PKI Platform管理者が、お客様に代わって PKI Platform管理者としての任務を果たす権限を取り消された場合、お客様はすみやかに当該PKI Platform管理者の管理者証明書の失効を要求するものとします。

お客様の利用者。お客様は、この取り決めに従って証明書を受け取る利用者に、適切な利用規約の条項に従わせる義務を持つものとします。また、利用者は、証明書の登録条件としてその利用規約に合意するものとします。お客様は、その利用規約の条項によって、CAに対してDigiCert Trust Network CPSの条項と同等の安全性を保証するものとします。

DigiCertの保証。DigiCertは以下の項目を保証します。(i) DigiCertが証明書作成の際に注意を怠ったために証明書の情報に誤りが入り込むような事態が起きないこと、(ii) DigiCertによる証明書の発行が、重要なすべての点においてDigiCert Trust Network CPSに準拠すること、(iii) DigiCertの失効サービスとリポジトリの使用が、重要なすべての点においてDigiCert Trust Network CPSに従うこと。

付録B: プライベート認証局

DigiCert PKI Platformでは、お客様がプライベート認証局（CA）から証明書を発行できます。Digicertは、セキュリティ保護された環境で厳密な手順に従って、このCAの秘密鍵/公開鍵ペアを生成します。この手続きはキーセレモニーと呼ばれます。これらの証明書は、通常、組織内のリソースへのアクセスを制御するために使用します。例えば、多くのお客様が、仮想プライベートネットワーク（VPN）の認証で自社のプライベートCAのみを信頼することで、社内ネットワークへの無断アクセスを防止しています。

標準パッケージでは、すべてのお客様がプライベートCAを自動的に利用できます。このCAの名義には、アカウントのセットアップ時にDigiCertに提示され、入念にチェックされた、お客様の正式な法人名が使用されます。自社の別の商標名（商標登録済みのブランド名など）を使用したい場合や、CAのデフォルト値を変更したい場合は、追加のCAを作成するオプションを購入することもできます。

注: お客様は、適用されるプライベート CA での証明書の発行、管理、使用に関する独自の認証局運用規定（CPS）を定義し、それに従う義務があります。

追加サービス条件 – プライベート認証局のみに適用

任命。お客様は、認可された1人以上のお客様側の従業員または信頼される者をPKI Platform管理者として任命する必要があります。任命されたPKI Platform管理者は、お客様に代わって追加のPKI Platform管理者を任命する権利を有するものとします。お客様は、この取り決めに従って証明書を受け取るPKI Platform管理者に、適用される利用規約の条項に従わせる義務を持つものとします。

管理業務。お客様は、DigiCert指定のハードウェアとソフトウェアを使用するお客様側の PKI Platform管理者を通して、証明書申請に含まれる情報を検証し、検証後の証明書申請を承認または却下して、DigiCertに発行を指示し、証明書の更新と失効を行うものとします。PKI Platform管理者が、お客様に代わってPKI Platform管理者としての任務を果たす権限を取り消された場合、お客様はすみやかに当該PKI Platform管理者の管理者証明書の失効を要求するものとします。

DigiCertの保証。DigiCertは、DigiCertが証明書作成の際に注意を怠ったために証明書の情報に誤りが入り込むような事態が起きないことを保証します。

付録C: Adobe® ドキュメントサイニングサービス

DigiCert PKI Platformでは、お客様がAdobe®ドキュメントサイニングサービス（CDS）から証明書を発行できます。DigiCertはAdobe社の協力の下で、Adobe Acrobat®、Reader®、LiveCycle®の各製品で自動的に信頼される証明書を発行できるようにしています。この証明書を前述の製品で使って、PDFにデジタル署名ができます。

標準パッケージでは、すべてのお客様が、シマンテック中間CA for Adobe CDSにつながる標準パッケージでは、すべてのお客様が、シマンテック中間CA for Adobe CDSにつながる発行元認証局（CA）を自動的に利用できます。このCAの名義には、アカウントのセットアップ時にDigiCertに提示され、入念にチェックされた、お客様の正式な法人名が使用されます。自社の別の商標名（商標登録済みのブランド名など）を使用したい場合や、CAのデフォルト値を変更したい場合は、追加のCAを作成するオプションを購入することもできます。

注: これらの証明書を発行、管理、使用するには、お客様とユーザーがAdobe CDS認証局運用規定（CPS）に準拠する必要があります。

AATLでは、お客様はSHA256またはECCを選択できます。

追加サービス条件 – Adobe®ドキュメントサイニングサービスのみに適用

任命。お客様は、認可された1人以上のお客様側の従業員または信頼される者をPKI Platform管理者として任命する必要があります。任命されたPKI Platform管理者は、お客様に代わって追加のPKI Platform管理者を任命する権利を有するものとします。

お客様は、この取り決めに従って証明書を受け取るPKI Platform管理者に、適用される利用規約およびCPSの条項に従わせる義務を持つものとします。

管理業務。お客様は、DigiCert指定のハードウェアとソフトウェアを使用するお客様側のPKI Platform管理者を通して、CPSに従って、証明書申請に含まれる情報を検証し、検証後の証明書申請を承認または却下して、DigiCertに発行を指示し、証明書の更新と失効を行うものとします。PKI Platform管理者が、お客様に代わって PKI Platform管理者としての任務を果たす権限を取り消された場合、お客様はすみやかに当該PKI Platform管理者の管理者証明書の失効を要求するものとします。

お客様の利用者。お客様は、この取り決めに従って証明書を受け取る利用者に、適切な利用規約の条項に従わせる義務を持つものとします。また、利用者は、証明書の登録条件としてその利用規約に合意するものとします。お客様は、その利用規約の条項によって、CAに対してCPSの条項と同等の安全性を保証するものとします。

DigiCertの保証。DigiCertは、DigiCertが証明書作成の際に注意を怠ったために証明書の情報に誤りが入り込むような事態が起きないことを保証します。

付録D: LTE証明書サービス

DigiCert LTE Base Station サービス（以下「LTES」または「サービス」）では、プライベート階層内でデバイスを通信事業者のLTE機器に統合するためのデバイス証明書を取得できます。お客様またはお客様の通信事業者は、CMP（Certificate Management Protocol）などのプログラム的なインターフェースを介してDigiCertにLTESの要求を送信します。

追加サービス条件 – LTE証明書サービスのみに適用

任命。お客様は、認可された 1 人以上のお客様側または通信事業者側の従業員を、その雇用先企業体のサービス管理者として任命するものとします。お客様は、この取り決めに従って管理者証明書を受け取るPKI Platform管理者に、その証明書に関連付けられた適用される利用規約の条項に従わせ、本サービス記述書に準拠し認可された合法的な目的にのみPKI Platform管理者証明書を使用させる義務を持つものとします。かかる利用者がサービス管理者としての権限を取り消された場合、お客様はすみやかに当該の管理者証明書の失効を要求するものとします。

管理業務。お客様とその通信事業者は、任命したPKI Platform管理者を通して、以下のうちの該当する業務の責任を持つものとします。

1. 通信事業者のサブアカウントの作成
2. 証明書プロファイルの作成
3. 製造元へのCA証明書の提供
4. 検証のためのIPアドレスブロックの提供
5. 新しいデバイスの登録と要求の事前承認の設定
6. ネットワーク構成要素のCMPレスポンダURLの設定

アカウントの認可と証明書の発行。お客様は、この取り決めに従って発行されたLTE証明書を受け取る権限を持つ通信事業者の事前認可を書面にてDigiCertに提供するものとします。この書類には、通信事業者の連絡先、サービス管理者として任命された人物の身元確認情報（登録に使用される情報を含む）、各通信事業者に認可されたLTE証明書と拠点の数などを記載します。お客様は、各PKI Platform管理者が、適用されるPKI Platform管理者証明書が作成されて以来、その証明書の秘密鍵、およびその秘密鍵を守るためのチャレンジフレーズ、PIN、ソフトウェア、またはハードウェアメカニズムを扱う唯一の人物であり、今後もそうであり続けること、ならびに認可されていない人物がこれらの情報やシステムにアクセスしたことがなく、今後もアクセスしないことを保証し、通信事業者にこれらを保証させる義務を持つものとします。

お客様が認可した数の証明書をPKI　Platform管理者がWebポータルから要求したとき、DigiCertは（i）各証明書要求に含まれる情報の正確性を信頼し、（ii）要求元のPKI　Platform管理者に対して証明書を発行および提供する権利を有するものとします。本サービス記述書の下で発行または許諾されたデバイス証明書は、証明書の発行日から1年、2年、または3年の証明書有効期間が定められます。DigiCertは、前述の要件に従って、すべての注文を受領順に履行します。本条件の条項と矛盾する場合でも、証明書を要求できる通信事業者の数、および証明書の要求元となる拠点とPKI Platform管理者の数は、適用されるサービス注文書で指定された数に厳格に制限されます。

製造元フローダウン義務。お客様は、DigiCertのシステムまたはソフトウェアの技術的実装を監視、妨害、リバースエンジニアリングせず、またはその他の方法でそれらのセキュリティを故意に侵害しないものとします。また、指定された製造元に対しても同様の義務を持つものとします。

CA証明書。本サービス記述書のいかなる反対の規定にかかわらず、DigiCertは、DigiCertの標準PKI手順とポリシーに従って、お客様の2つのルート証明書、およびオプションで各ルート証明書の下で発行される最大2つまでのCA証明書を作成およびホストします。このCA証明書は、この取り決めに従ってお客様に本サービスを提供することのみを目的としています。追加のCA証明書は別途購入できます。DigiCertは、お客様からの要求に基づき、標準のPKI手順とポリシーに従って通信事業者を本サービスに追加し、そのサブアカウントを作成します。

IPアドレス設定。新しい通信事業者を追加する際に、有効なIPアドレスの範囲をDigiCertに提供する必要があります。DigiCertのシステムは、有効なIPアドレスから送られたCMP要求にのみ応答し、それ以外のIPアドレスから送られた要求はすべて拒否します。この設定は、通信事業者側で実行されなければなりません。

アカウントの有効化。サービス注文書を通した料金の前払いを前提として、（i）必要な登録手続きの完了、（ii）通信事業者とそのPKI　Platform管理者の認証という要件が満たされた時点で、DigiCertは、米国内では10営業日以内、米国外では商業上道理にかなった期間を基準に、商業上道理にかなった労力を費やしてサブアカウントを有効化するものとします。DigiCertが認証手続きを滞りなく行えるように、この期間中、PKI Platform管理者は常に連絡可能であることが求められます。

DigiCertの保証。DigiCertは、DigiCertが証明書作成の際に注意を怠ったためにここで発行された証明書に誤りが入り込むような事態が起きないことを保証します。

付録E: 製造元証明書

DigiCert PKI Platformでは、製造元のエコシステム固有のデバイスに統合するために、プライベート階層から製造元証明書を発行できます。製造元証明書は、デバイスの認証またはデバイスから送信されるメッセージの暗号化に使用されます。お客様は、バッチインターフェイスを使用して、DigiCert PKI Platformから製造元証明書を申請します。

追加サービス条件 – 製造元証明書のみに適用

任命。お客様は、認可された 1 人以上のお客様側の従業員を、その雇用先企業体のPKI Platform管理者として任命するものとします。お客様は、この取り決めに従って管理者証明書を受け取るPKI Platform管理者に、その証明書に関連付けられた適用される利用規約の条項に従わせ、本サービス記述書に準拠し認可された合法的な目的にのみ管理者証明書を使用させる義務を持つものとします。かかる利用者がサービス管理者としての権限を取り消された場合、お客様はすみやかに当該の管理者証明書の失効を要求するものとします。

管理業務。お客様とその通信事業者は、任命したPKI Platform管理者を通して、以下のうちの該当する業務の責任を持つものとします。

1. サブアカウントの作成
2. 証明書プロファイルの作成
3. 製造元CA証明書の提供
4. 証明書発行のバッチ申請の送信

製造元フローダウンの義務。お客様は、DigiCertのシステムまたはソフトウェアの技術的実装を監視、妨害、リバースエンジニアリングせず、またはその他の方法でそれらのセキュリティを故意に侵害しないものとします。また、指定された製造元に対しても同様の義務を持つものとします。

証明書の発行。サービス管理者がPKI Managerからの証明書のバッチ申請の送信時に、DigiCertは (i) そのような証明書申請書の情報の正確性に依拠する権利を有します。(ii) 申請しているPKI Platform管理者に当該証明書を発行し提供する権利を有します。DigiCertは、前述の要件に従って、すべての注文を受領順に履行します。本書の矛盾する条項にかかわらず、申請できる証明書の数は、適用されるサービス注文書で指定された数に厳格に制限されます。

アカウント有効化。サービス注文書を通した料金の前払いを前提として、（i）必要な登録手続きの完了、（ii）顧客とそのPKI Platform管理者の認証という要件が満たされた時点で、DigiCertは、米国内では10営業日以内、米国外では商業上道理にかなった期間を基準に、商業上道理にかなった労力を費やしてアカウントを有効化するものとします。DigiCertが認証手続きを滞りなく行えるように、この期間中、PKI Platform管理者は常に連絡可能であることが求められます。

DigiCertの保証。DigiCertは、DigiCertが証明書作成の際に注意を怠ったためにここで発行された証明書に誤りが入り込むような事態が起きないことを保証します。

プライベートルート認証局に必要な条件。製造元証明書はルート認証局のプライベート階層で稼働するため、DigiCertがホストするルート証明書の下に発行された製造元証明書を受領するための前提条件として、ルート認証局が課すすべての条件を満たす必要があります。ルート認証局が業界団体や標準設定機関など、お客様以外の第三者である場合、製造元証明書は、そのようなルート認証局によって管理されるエコシステム内でのみ使用されることを意図しています。そのような前提条件には、ルート認証局が指定する追加文書の実行が含まれますが、それに限定されません。**ルート認証局は、エコシステムへの製造元証明書の発行において絶対的な権限を持ち、お客様に証明書を発行しないようにDigiCertに指示する権利を留保します。DigiCertは、ルート認証局の対応に関連するあらゆる責任を負わないものとします。ルート認証局は、エコシステムの各製造元証明書で所有しているあらゆる所有権および知的財産権を保持します。ルート認証局が所有するそのような権利は、ルート認証局の指定するドキュメントに従ってお客様にライセンスが付与されます。お客様は、ルート認証局の要請に応じて、DigiCertがお客様の身元情報と証明書の販売に関する情報を報告しなければならない場合があることを承認し、同意するものとします。**

詳細情報

製品についてのお問い合わせ:

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