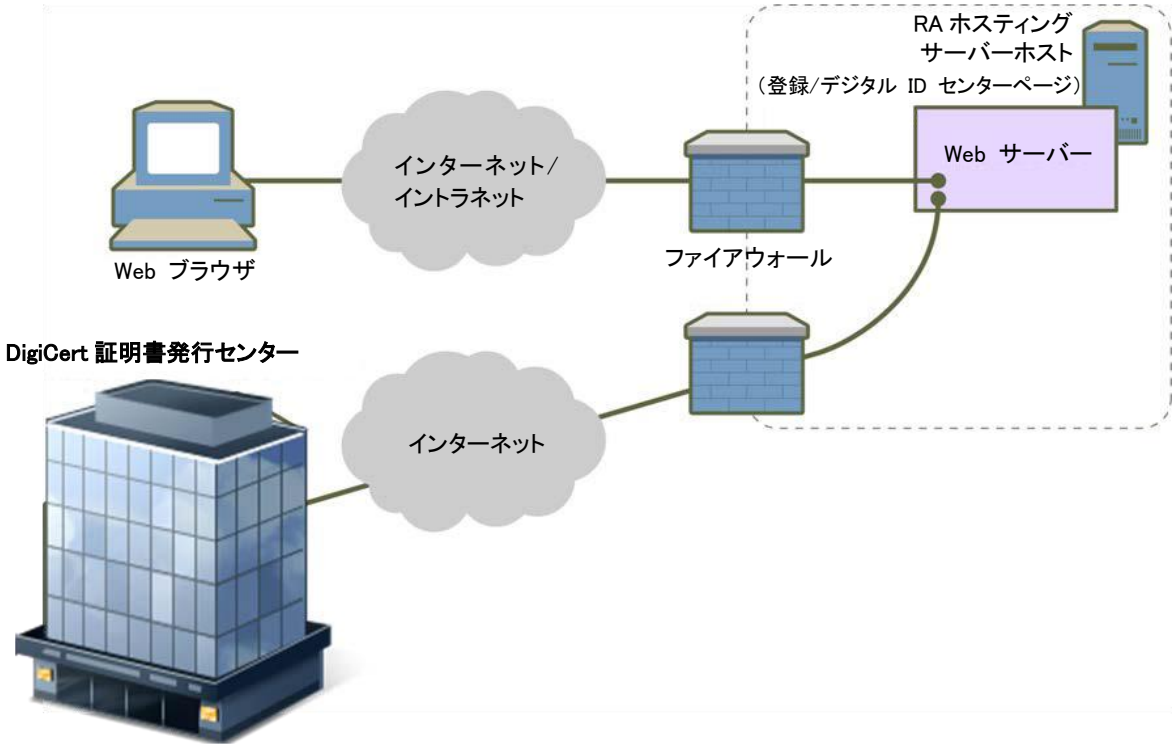
DigiCert PKI Platform RA ホスティングサービス記述書

はじめに

DigiCert PKI Platform RA ホスティングサービスは、DigiCert PKI Platform 7.x バージョンにおいて、証明書の新規申請や更新を受け付けるためのオンライン受付サイトの RA コンテンツを提供します。本サービスは DigiCert のデータセンターサーバーに Web ページをホストするサービスです。

図 1 RA ホスティングサービス構成
注: 点線内のシステムが本 RA ホスティングサービスに該当します。



主要機能

- PKI Platform デジタル ID センター
  デジタル ID センターページは、エンドユーザー証明書の登録を受け付けるページで、PKI Platform サービスにおける**ローカルでのホスティングを選択し、かつ DigiCert のデータセンターに設置する RA ホスティングサービス**（**図 1**）を選択した場合は、お客様の作成するコンテンツを DigiCert の Web サーバーで管理します。どちらでホストする場合でも、証明書の発行は DigiCert が行います。コンテンツの作成条件は DigiCert PKI Platform（7.x）以前のローカルホスティングに準じます。

- 認証方法
  RA ホスティングサービスを利用した DigiCert PKI Platform Service では、手動認証、パスコード認証のいずれかの方法で要求を認証および承認できます。自動承認による認証は選択できません。

  手動認証
  手動認証では、管理者が証明書要求を 1 つ 1 つ審査して、承認または却下します。管理者の負担が大きくなるため、証明書の発行数が多い組織にはあまり適していません。

  パスコード認証
  パスコード認証では、証明書要求の認証を自動化できます。管理者は、PKI Platform コントロール

センターでパスコード認証の設定を行います。利用者が証明書を要求すると、管理者が TLS 通信を通じて、事前に DigiCert にアップロードされた登録情報と照合されます。組織が定める承認基準に従って、証明書要求が承認または却下されます。自動認証とは異なり、パスコード認証では、お客様側で認証サーバーを構築および管理する必要はありません。認証はすべて、管理者がアップロードした利用者データに基づいて DigiCert 側で行われます。そのため、パスコード認証は自動認証に比べて実装が簡単ですが、柔軟性はやや劣ります。

- 上記以外の PKI Platform の機能について
  DigiCert PKI Platform サービス記述書（バージョン 7．x およびそれ以前）に準じます。

付録 A – PKI Platform RA ホスティング利用規約

1. 定義

「管理者証明書」とは、PKI Platform 管理者として指定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 Platform コントロールセンター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。(a) 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 (b) 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。

「契約」とは、DigiCertとお客様の間で結ばれ、本サービス記述書に適用されるサービス注文書が発行された、プロフェッショナルサービス契約またはその他のマスター契約や規約を指します。

「証明書」または**「デジタル証明書」**とは、少なくとも発行元 CA の名前または識別情報、利用者の識別情報、利用者の公開鍵、証明書有効期間、証明書のシリアル番号、発行元 CA のデジタル署名を含むメッセージを指します。

「証明書申請者」とは、CA に証明書の発行を要求する個人または委任代理人を指します。**「証明書申請」**とは、証明書申請者（または委任代理人）から CA に提出される証明書発行要求を指します。

「証明書署名ユニット」または**「CSU」**とは、証明書への署名と鍵の保管用に設計されたハードウェア装置またはソフトウェアを指します。

「認証局」または**「CA」**とは、証明書を発行、停止、失効する権限を持つ個人またはエンティティを指します。

「認証局運用規定」または**「CPS」**とは、CA または RA 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。DTN CPS は、DigiCert Web サイトのリポジトリで公開されています。

「誤発行」とは、(a) DTN 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。

「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。

「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。

「証明書有効期間」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、それより後の特定の日時）から、有効期限が切れる日時または失効が実行された日時までの期間を指します。

「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化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化できます。

「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。

「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。

「利用者」とは、証明書の主体であり、発行対象である、個人またはエンティティを指します。利用者は、発行時に証明書に含まれる公開鍵に対応した秘密鍵を使用でき、使用する権限を持ちます。

「信頼される者」の定義は、CPS での定義に従います。**「DigiCert Trust Network」**または**「DTN」**とは、DigiCert Trust Network 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（PKI）を指します。DigiCertとその関連会社、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。

2.提供内容

本サービスによる業務範囲を以下に記します。

(a) お客様が用意する RA コンテンツの、DigiCertが用意するウェブサーバーへ展開、保存、Web サイトの設定。

（b） 構築された環境の運用。

(c) 運用範囲

本サービスは別途定める時間帯を除き、本サービス提供のために必要なシステムを、原則として 24 時間稼働します。またその運用範囲以下とします。

・サーバー運用

サーバー監視（死活監視、プロセス監視）

日次差分／週次フルバックアップ
バージョンアップ、脆弱性対策（パッチ適用等）
サポートサービス記述書にしたがったサポート
・不正侵入検知
24 時間の不正アクセス監視
バージョンアップ、脆弱性対策（パッチ適用等）
1 営業日以内の障害対応
・ファイアウォール
共用ファイアウォール
バージョンアップ、脆弱性対策（パッチ適用等）
1 営業日以内の障害対応
セキュリティチェック
サービス導入時に稼働プロセスのセキュリティホールを診断
なお以下については DigiCert にて決定、運用されます。
・障害時代替機
・ウェブサーバーのホスト名、ホストの TLS サーバ用 ID

本サービスにおいて DigiCert の指定するログについては、原則お客様に提供しません。
バージョンアップ、脆弱性対策作業についてはメンテナンス実施時に行います。
DigiCert の用意するウェブサーバーはお客様間での共有サーバーとなりますので、原則 1 CA、1 ディレクトリをお客様専用のディレクトリとして割り当てます。

3. サービス提供の中断

システム・メンテナンス、バックアップおよび機能のアップグレードを行うために、毎週 6 時間を上限として本サービスの提供を中断し、本サービスの中断時間は、PKI Platform 管理者宛てに通知します。
メンテナンス時間
毎週土曜日 0:00～4:00
1 週間に 6 時間を超えて本サービスを中断する必要がある場合、お客様に同様の方法で予め通知します。
また次のいずれかの場合に、DigiCert は本サービスを中断または提供中止をすることがあります。この場合お客様に同様の方法で予め通知いたします。
（a）天災、地変、その他の非常事態が発生した場合
（b）DigiCert の管理する設備もしくはシステムの保守を緊急に行う必要がある場合
（c）TLS サーバーID の新規取得、更新、入れ替えに必要となる作業が必要である場合
（d） その他 DigiCert が必要と認めた場合

4, ログの提供

お客様は障害及び調査目的で DigiCert の用意するウェブサーバーのアクセスログを要求することができます。この場合その都度取得したいログ出力帯（YYYY/MM/DD HH:MM:SS～YYYY/MM/DD HH:MM:SS を指定 ）、障害内容及び調査事項を明記の上調査依頼を行うことができます。
DigiCert は原則として、ログ提供希望日の 3 営業日以上前に要求を受付けます。（要求時に併せてアクセス元の IP アドレス等情報を明記することが望ましいものとします）
ファイル提供は管理者宛てへの電子メール宛てに送付するものとします。
なお、以下は原則として提供いたしません。
・期間を特定しない日常的なログの提供
・アクセスログ以外のログ

5. コンテンツについて

RA ホスティングのコンテンツの編集、修正は原則としてお客様が実施するものとします。

6. そのほかの事項

本項以外の事項はサービスの本体となる PKI Platform のサービス記述書に従うものとします。