digicert®

10倍の規模に備えたWebPKIのアップグレード

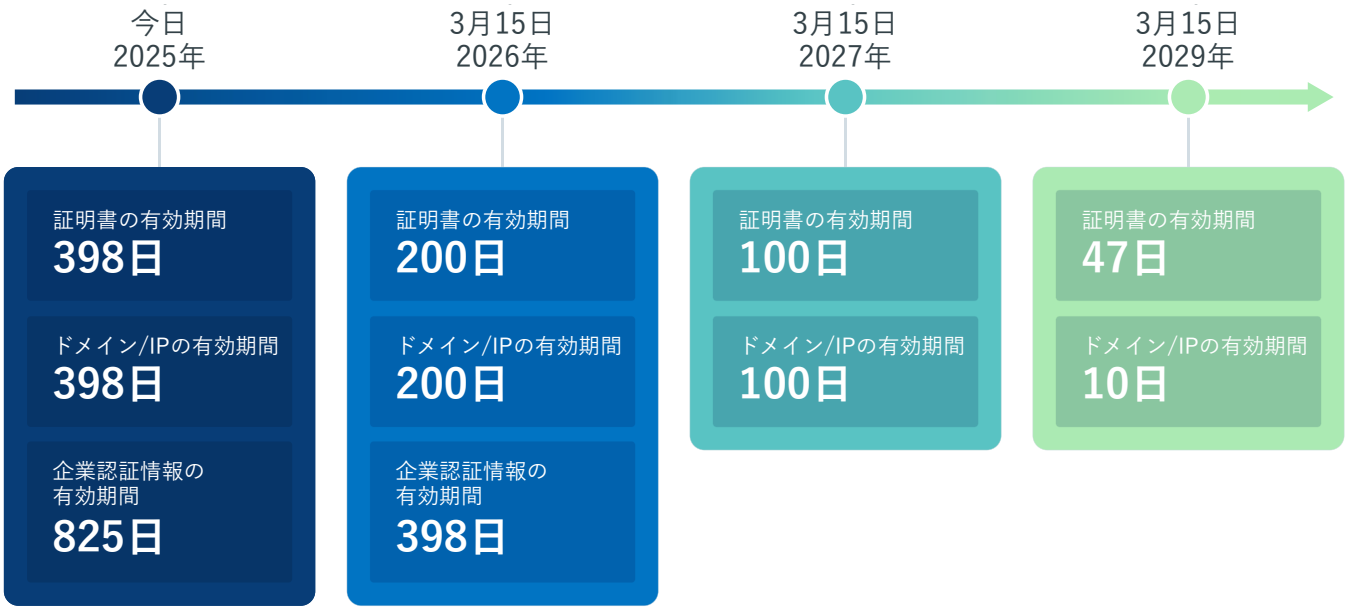
企業に必要な次世代のトラストインフラと運用に対して、デジサートが投資する理由

WHITE PAPER

概要

世界の公開鍵基盤（PKI）エコシステムは、これまでの10年以上の中で、で最も重要な変革期を迎えています。CA/Browser Forumのポリシー変更により、2029年3月15日までにTLS証明書の有効期間は398日から47日に短縮されます。ドメイン名およびIPアドレス認証情報の有効期間は398日からわずか10日に短縮されます。その結果：

- 発行される証明書が8倍必要になる
- ドメイン認証は40倍必要になる
- 組織は自動化を推進しなければ、広範なサービス停止やセキュリティ侵害のリスクに直面する
- PKIプロバイダーはインフラ、セキュリティ制御、運用を大規模に拡張する必要がある



証明書は **8倍** ドメイン認証は **40倍** 必要になります

このホワイトペーパーでは、デジサートがインフラストラクチャ、暗号技術、コンプライアンス、自動化、運用にわたる総合的な近代化への取り組みについて説明します。取り組みにより、1日あたり10倍のパブリック証明書の発行、グローバルなトラストの確保、企業、政府、公共インターネット向けに安定的なデジタルセキュリティの提供が可能となります。

インフラストラクチャのスケールを10倍化

デジサートは、パフォーマンス、可用性、セキュリティを損なうことなく、大幅に増加したパブリック証明書の発行と管理を可能にするため、エンタープライズWebPKIインフラストラクチャを大きく拡大し、コンピューティング、暗号技術、世界規模での配信を強化しています。

コンピューティング、ストレージ、HSMへの投資

10倍に膨れ上がる証明書の発行量に対応するため、デジサートは署名処理を支える中核的な暗号処理基盤とコンピューティング基盤を強化しています。これらの投資により、グローバルなトラストサービスに必要なパフォーマンス、耐久性、拡張性が確保されます。

- 証明書の並列発行に最適化された高性能署名クラスター
- 安全かつコンプライアンスに準拠した鍵保護のための冗長化されたグローバルHSMネットワーク
- 大規模PKIワークロード向けた次世代コンピューティング・ストレージ・分析フレームワーク
- パフォーマンスの低下なくグローバルな急増を吸収する弾力的なスケーリングアーキテクチャ

これらの強化により、証明書需要の急激な増加に対応するために必要な暗号処理スループットと低遅延性能を実現します。

WebTrust準拠データセンター内のゾーニング

継続性と障害箇所の隔離を強化するため、デジサートは物理的な監査を通ったWebTrust準拠のデータセンター内に複数の可用性ゾーンを実装しています。これらのゾーンにより、同一リージョン内での独立した運用とフェイルオーバーが可能となります。

この設計は、負荷増加下でも大幅に高い可用性を実現し、デジサートのSLAに既定の99.99%稼働率を保証します。

Multi-Perspective Issuance Corroboration（MPIC）

DNS 脅威が世界的に拡大する中、デジサートは複数の地理的に独立したネットワーク拠点からドメイン名の利用確認 (DCV) および認証機関認可 (CAA) チェックを実行しています。

- 汚染された DNS キャッシュ応答を検出
- ISPまたはラストマイル経路の改ざんを特定
- 地域的な中間者攻撃（MITM）をブロック
- 非対称または不整合な権威DNS応答を防止

このMPIC アプローチは証明書発行の完全性を大幅に強化し、地域固有のDNS攻撃から顧客を保護します。

耐量子コンピュータ暗号（PQC）への投資

耐量子コンピュータセキュリティへの移行に備え、デジサートはインフラ全体に次世代PQC機能を配備しました。これにより企業は、ハイブリッド型および純粋なPQC対応の証明書を今すぐ導入できます。

- より大きな鍵サイズを扱えるPQC対応HSM
- 次世代証明書のチェーンを支える専用PQCプライベートルート
- NIST承認のPQC暗号アルゴリズムを全てサポートし、高性能な最適化を実現
- ハイブリッドおよび純粋なPQC証明書の本格的な発行

デジサートは、お客様とそのエコシステムを数十年にわたり保護するために設計された、量子コンピュータへの耐性をもつトラスト基盤を構築しています。

CT、OCSP、CRLインフラの強化

発行量が増加するにつれ、証明書の透明性ログ（CTログ）、オンライン証明書ステータスプロトコル（OCSP）、および証明書失効リスト（CRL）システムもそれに応じて強化する必要があります。これらのサービスは、ブラウザやサーバーが証明書の真正性と失効ステータスをリアルタイムで検証できるようにします。

- 高負荷対応の分割化・冗長化されたCTログインフラストラクチャ
- OCSP応答とCRLの両方に対するグローバルエッジ配信
- 異常を迅速に検出するための高度な監視およびアラート機能
- 冗長化され地理的に分散されたインフラによるサービスの中断防止

これらの強化により、世界中で予測可能で高速かつトラスト性の高い証明書ステータス確認が保証されます。

グローバルなパフォーマンスと障害耐性を実現するマルチCDN構成

信頼性のあるアーティファクトを世界中で 100 ミリ秒未満で確実に利用できるように、デジサートは マルチCDN 戦略を用いてエッジロケーションを拡大しました。これにより、すべてのグローバル地域で最高の速度、冗長性、安定性を提供します。

- 世界的なカバレッジを実現する複数のTier-1 コンテンツ配信ネットワーク（CDN）
- 最寄りのエッジからの応答配信のための自動化された地理的ルーティング
- 配信経路に統合されたネイティブDDoS保護
- エッジロケーション全体での統一されたOCSP応答配信
- CTログおよびCRLの安定的な配信

この多層アーキテクチャにより、すべてのトラストサービスにおいてワールドクラスのパフォーマンスと障害耐性が保証されます。

30以上のグローバルデータセンターにおけるアップグレード

デジサートは、地域ごとのコンプライアンス要件、越境データ制限要件、低遅延のトラスト性提供をサポートするため、30以上のグローバルデータセンターにまたがるインフラの近代化を進めています。これらのアップグレードには、コンピューティング、トランジット、ネットワーク、電力の冗長性の改善が含まれ、米国、EU地域、日本、オーストラリア、インドの施設に広がっています。これらのグローバルな投資により、お客様がどこで事業を展開していても、より高速で信頼性が高く、地域ごとのコンプライアンスに準拠したトラストサービスが保証されます。

デジサートのサポートと運用を強化

ワールドクラスのインフラにはワールドクラスの運用効率が不可欠です。デジサートはサポート、コンプライアンス、クラウド運用を近代化し、10倍の運用需要に対応します。

AIによる企業認証（OV）およびEV認証の強化

証明書の有効期間が短縮される中、企業認証（OV）およびEV認証の速度と正確性が極めて重要となっています。デジサートはAIを活用し、認証プロセスの効率化、エラーの低減、グローバル規模での発行までの時間短縮を実現します。

- AIによる事業登録確認の迅速化
- 自動照合による身元・法人確認
- 機械学習モデルによる文書抽出・解析・分類
- 自動化されたエンティティ確認とヒューリスティクス検証
- 発行の安全性をもたらすAI駆動型不正・異常検知の仕組み

これらの強化により、業界の基準要件を上回る、認証時間の大幅な短縮化と精度の向上を実現します。

オープンソースのドメイン利用権確認

ドメイン名の利用権確認（DCV）は、TLS発行におけるトラストの基盤です。デジサートはオープンソースDCVライブラリによって自動化に対応した基盤を提供し、一貫性をもたらすことで顧客と業界全体のセキュリティを強化します。

- 全DCV方式に対応した標準化された認証ロジック
- DNSおよびHTTPを使った認証メカニズムの強化
- エコシステム向けの透明性が高く検証可能な実装
- エンタープライズ規模の展開に向けた自動化対応ツール

このアプローチにより、大規模な運用を行う顧客に対して一貫性のある安全なドメイン名の認証のシステムを提供し、自動化を加速します。

グローバルサポートとサービスの強化

証明書のライフサイクル短縮化により、顧客との接点と運用負荷が増加しています。発行量と自動化の需要が急速に拡大する中、デジサートは高品質なサービスを保証するため、グローバルサポート体制を拡大しています。

- 技術サポート要員とシステムの拡充
- カスタマーサクセスおよびソリューション導入チームの強化
- エンタープライズ導入向けプロフェッショナルサービスの強化
- 専門的なPKI運用とコンプライアンスエンジニアリング

これらの投資により、証明書更新サイクルが加速する中でもワールドクラスのサポート品質を保証します。

AIを活用したナレッジ&セルフサービスシステム

グローバルなPKIの複雑化が進む中、お客様は正確なガイダンスへの即時アクセスを必要としています。デジサートはプラットフォーム全体にAIを導入し、人間の介入を必要としないインテリジェントで文脈に応じたヘルプを提供します。

- DigiCert ONEに組み込まれたAIガイダンス
- リアルタイムトラブルシューティングのためのAIサポートアシスタント
- 社内およびコミュニティコンテンツを活用したAIキュレーション型ナレッジベース
- 状況認識型の診断・解決ワークフロー
- 一般的なPKI、DNS、ライフサイクルタスク向けのガイド付き自動化

これらのシステムは顧客体験を向上させ、デジサートが業界トップクラスのNPSを80以上維持するという目標を支えています。

コンプライアンスの自動化による監査の強化

インフラストラクチャと発行規模の拡大に伴い、監査の対象も拡大します。デジサートは年間 30以上の監査を受けており、運用上のボトルネックなく信頼性とコンプライアンスを維持するために、監査準備の自動化を進めています。

- システム全体にわたる自動化された証拠収集
- 構造化された統制とポリシーのマッピング
- 監査人レビューのためのAIベースのサンプリング
- コンプライアンス管理の継続的監視

デジサートは、ISO 27001および米国 FedRAMPの認証を取得し、最も信頼されるグローバル認証機関としての地位を強化しています。

クラウド運用自動化

10倍のスケールを実現するには、自動化、モニタリング、安全なデプロイメント手法に基づくクラウド運用モデルが必要です。デジサートのサイトリライアビリティエンジニアリング（SRE）チームは、クラウドシステムを近代化し、世界中で一貫したゼロダウンタイムのサービスを提供しています。

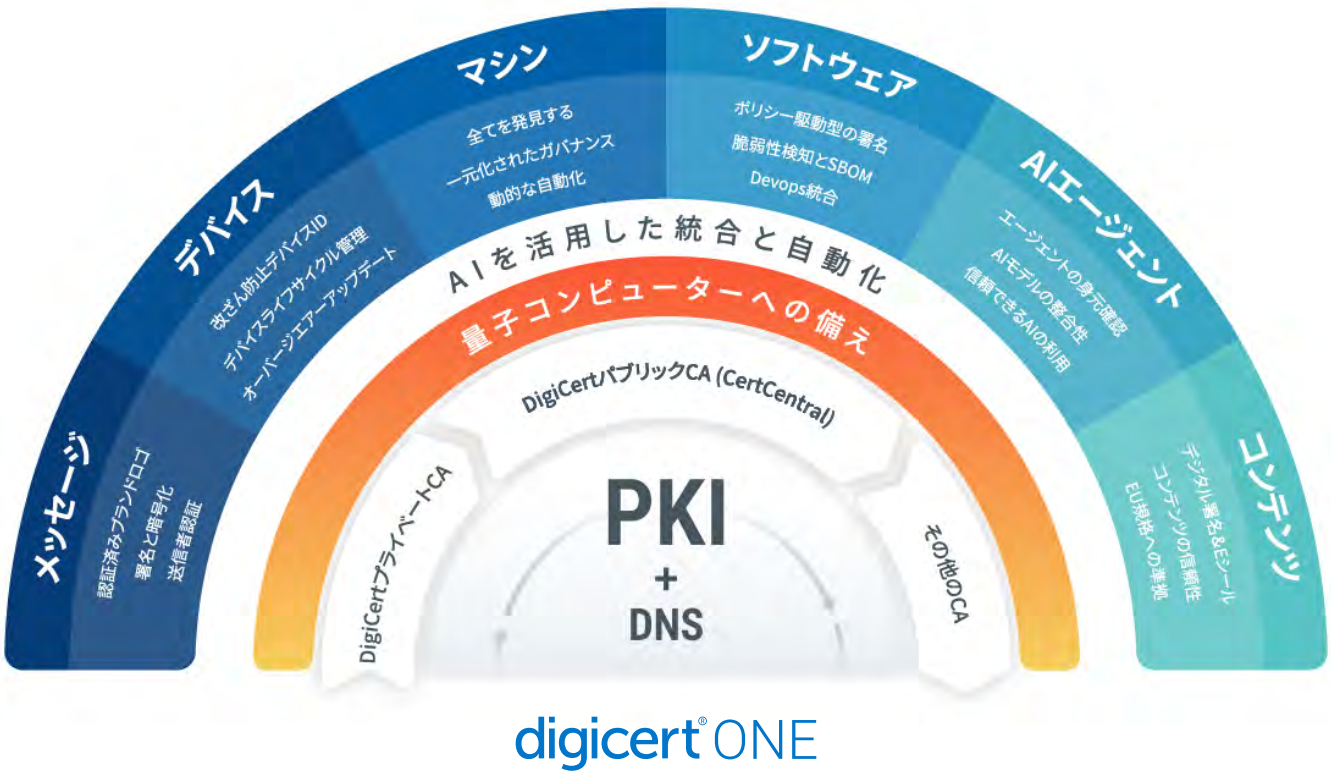
- 迅速かつ安全なリリースを実現するCI/CDパイプラインの強化
- Blue - Green およびCanaryデプロイメントアーキテクチャの採用
- トラスト性の高いプロビジョニングのためのインフラストラクチャ・アズ・コードガバナンス
- インシデント防止のためのSRE作成自動化プレイブック
- リアルタイムログ・メトリクス・トレースによる深い可観測性

これらの投資により、グローバルな稼働率と一貫したプラットフォームの信頼性を維持しながら、継続的な改善が可能になります。

顧客にレジリエンスを提供

証明書の有効期間が短縮され、更新頻度が急増する中、環境の安全性と可用性を維持する唯一の信頼できる手段は自動化です。デジサートはプラットフォームのあらゆる層に自動化を組み込み、お客様の手動更新リスクを排除し、運用コストを削減し、障害発生を未然に防げるようにします。

すべてのデジサートパブリックTLS/SSL証明書には、証明書発行と更新を自動化する業界標準プロトコルであるACME（Automated Certificate Management Environment）をデフォルトでサポートしています。デジサートのACMEサービスを利用すれば、お客様はデジサート組み込みのACMEクライアントまたはACMEv2準拠の任意のクライアント（例：Certbotやwin-acme）を使用して、CertCentralから直接証明書を発行・インストールできます。ACME認証情報が設定されると、クライアントはバックグラウンドで継続的に証明書のライフサイクルイベントを管理し、有効期限切れ前に証明書を更新し、サポート対象のエンドポイントに展開します。これにより、TLS管理のオーバーヘッドと人的ミスが大幅に削減されます。



digicert® ONE

DigiCert ONE は、この自動化モデルをパブリックTLSを超えて拡張し、SaaSサービスとしてあらゆるエンタープライズPKIおよびDNS利用ケースに対応する統合プラットフォームを提供します。最新のコンテナベースアーキテクチャを基盤とするDigiCert ONEは、あらゆる環境において、マシン、ソフトウェア、IoTデバイス、サービス、コンテンツを横断して、スケーラブルで拡張性のある自動化された証明書ライフサイクル管理と権威DNSを実現します。クラウド、オンプレミス、ハイブリッド、エアギャップ環境での展開に対応します。DigiCert Trust Lifecycle ManagerとそのAPIを通じて、企業は内部・外部サーバー、ワークロード、VPN、WiFi、ネットワークアクセス、アプリケーションインフラを保護するパブリック/プライベートPKI証明書の検出、発行、更新、失効処理を自動化可能。UltraDNSとの統合により、DNSとPKIを単一の運用フローに統合します。この統一されたポリシー駆動型自動化基盤は、セキュリティリスクの低減、サービス停止の防止、コンプライアンスの確保を実現し、WebPKI規模での運用に必要なフェイルセーフ基盤を提供します。

おわりに

WebPKIの変革は、大幅に短縮された証明書の有効期間、継続的な検証要件、量子コンピュータ時代の暗号技術の台頭によって推進され、数十年にわたるデジタルトラストにおける最も破壊的な転換点となります。これらの変化に対応するには、漸進的な改善以上のものが必要です。証明書のライフサイクル全体にわたり、規模、自動化、レジリエンス、AIの再構築が求められます。デジサートは時代を先取りした投資を行い、10倍の発行パフォーマンス、世界規模でのマルチゾーン冗長性、MPIC、量子コンピュータ耐性を備えた暗号技術、AIを活用した自動化運用モデルを実現しています。この次世代型プラットフォームにより、デジサートはトラスト要件が年々加速する中でも、組織が自社システムを停止やコンプライアンスリスク、不要な運用負担なしに安全かつ継続的に運用することを可能にします。デジサートはWebPKIの未来に適応するだけでなく、その未来を先取りし、インターネットの次なる時代に向けたインテリジェントで自動化された、世界規模で障害耐性のあるトラストインフラを提供します。