DigiCert® Solutions
Infrastructure Security

digicert®

DigiCert® Solutions インフラセキュリティ

フォーチュン 500 およびグローバル 2000 の企業は、デジサート の 14 年以上にわたるハイアシュアランス TLS/SSL、PKI、IoT、署名ソリューションなどのデジタルトラストソリューションを、世界中の数百万のユーザーおよびデバイスに提供してきた経験に信頼を寄せています。

デジサートのソリューションには、DigiCert ONE、PKI Platform、eIDAS[1]-に準拠したQWAC（Qualified Website Authentication Certificates）などがあります。これらのソリューションは、オンプレミス、クラウド、ハイブリッド実装など、さまざまなビジネスニーズに対応するように設計されている。デジサートが管理するソリューションは、高可用性とフォールトトレランスのために設計されているだけでなく、厳格なセキュリティプロセスと標準に準拠したセキュアなインフラストラクチャ上で実行される。

デジサート のセキュアなインフラストラクチャを利用して、認証、暗号化、および電子署名のニーズに対して、企業が必要とするパフォーマンス、信頼性、およびセキュリティを提供します。

主な機能

厳格な物理、システム、ネットワークセキュリティ

デジサート のクラウド実装におけるセキュアなインフラには、以下のような特徴があります：

- 物理セキュリティインフラ：生体認証アクセス制御を含む多要素認証。檻の中での物理的ルールとして常時2名作業による相互監視。システムへ物理的にアクセスするには、複数のセキュリティゾーンが必須。
- 信頼できる社員のみのアクセス制限：デジサートのインフラにアクセスできるのは、徹底した身元審査に合格したデジサート社員のみ。
- 安全な鍵管理：暗号鍵は、FIPS 140-2 準拠の専用HSM（ハードウェア・セキュリティ・モジュール）上で暗号化された形式で保存。
- システムとネットワークセキュリティ：セキュリティ業界のベストプラクティスを採用するだけでなく、DDoS、ウェブアプリケーション攻撃、リソース攻撃、およびその他の広範な保護から保護するためのセーフガードを実装。
- 役割ベースの管理：すべてのITサービスは、担当者間の職務を分離し、機密情報や機能への個人アクセスを防止。

高可用性

デジサートの安全なインフラは、米国、日本、オーストラリア、ヨーロッパの各地域のデータセンターにホストされています：

- 冗長電源と冷却システム：冗長冷却に加え、すべてのIT機器は二重電源で、複数の独立した配電経路から供給。
- 地理的分散：すべての重要なウェブインフラをグローバルにロードバランシング。
- 冗長インフラ：すべての重要なネットワークとシステムコンポーネントはフォールトトレラント。

継続的なグローバル・モニタリング

- 専用の監視：デジサートネットワークオペレーションセンターは、デジサートのインフラ、システム、ネットワークを24時間365日体制で監視。
- 第三者による監視：デジサートは、重要なインフラ、システム、およびネットワークを監視するために、外部のサードパーティのグローバルサービスを採用。
- 信頼できる社員のみのアクセス制限：デジサートのインフラにアクセスできるのは、徹底した身元審査に合格したデジサート社員のみ。
- 安全な鍵管理：暗号鍵は、FIPS 140-2 準拠の専用HSM（ハードウェア・セキュリティ・モジュール）上で暗号化された形式で保存。

[1]Electronic IDentification, Authentication and trust Services（電子識別、認証、およびトラストサービス）
[2]Federal Information Processing Standards（連邦情報処理標準　または　連邦情報処理規格）

独立機関による監査と認証

デジサート独自の広範な情報セキュリティポリシーおよび慣行に加え、デジサートのソリューションは、独立した第三者により定期的に監査され、以下を満たしています：

適用: 全世界

製品/スキーム	監督機関	トラストサービスの要件	認証機関／監査人	詳細	適用
SSAE-16 SOC 2 Type II および III	AICPA[3]	セキュリティ、可用性、処理の完全性、機密性、プライバシーの5つの「トラストサービス原則」に基づき、顧客データを管理するシステムの運用上の有効性を詳述する。	BDO 米国	組織と顧客の利益を守るため、データが安全に管理されていることを確認するための年次監査。SOC 2は、従来のSAS 70報告基準に代わるものとなる。	全世界
WebTrust™ for Authorities	AICPA/CICA[4]	認証局が導入する管理の適切性と有効性。	BDO (DigiCert) EY (QuoVadis)		全世界
WebTrust™ for Baseline Requirements with Network Security		CA/B フォーラム[5]「パブリックで信頼される証明書の発行と管理のための基本要件」		DigiCert のパブリックおよびマネージド PKI CA サービスにおける鍵管理とビジネスプラクティスの開示に対して実施される年次監査。	全世界
WebTrust™ for Extended Validation		CA/B フォーラム “EV[6] 証明書の発行と管理のためのガイドライン”			全世界
WebTrust™ for Code Signing		コードサイニング・ワーキング・グループによる、「パブリックで信頼されるコードサイニング証明書の発行と管理に関する基本要件」。			全世界
WebTrust™ for IoT Matter		標準化団体（Connectivity Standards Alliance [CSA]）が定義する Matter PKI証明書ポリシー要件に基づく。	BDO (Digicert)	デジサート の鍵管理および証明書のライフサイクル管理業務、認証局の業務慣行の開示、および デジサート のマネージド PKI CAサービスをサポートする CA の環境管理に対して実施される年次監査。	全世界
WebTrust™ for CA (AATL 2.0)		Adobe 承認済みトラストリスト（AATL2.0）証明書の認証および発行に関する 認証局要件に準拠。	BDO (Digicert)	デジサート の鍵管理および証明書のライフサイクル管理業務、認証局の業務慣行の開示、および デジサート のマネージド PKI CAサービスをサポートする CA の環境管理に対して実施される年次監査。	全世界
WebTrust™ for VMC		認証マーク証明書（VMC）の発行に必要な最低限のセキュリティ要件に基づく。	BDO 米国	デジサート による認証マーク証明書（VMC）の発行に関する年次監査	全世界

[3]American Institute of Certified Public Accountants（米国公認会計士協会 ）
[4]Canadian Institute of Chartered Accountants（カナダ勅許会計士協会）
[5]CA/B Forum
[6]Extended Validation

適用: アメリカ

製品/スキーム	監督機関	トラストサービスの要件	認証機関／監査人	詳細	適用
FISMA[7]	OMB[8]	NIST[9] SP800-53, FIPS 199, FIPS 200	DataLock	最新のセキュリティ計画、文書化された管理、リスクアセスメントを確保するために、毎年セキュリティレビューを実施する。年3回の再認証が必要。	アメリカ合衆国
Federal PKI Shared Service Provider Program:	Federal Public Key Infrastructure Policy Authority (連邦公開鍵基盤ポリシー機関：FPKIPA) and General Services Administration (一般調達局：GSA[10])	NIST SP800-53は、米国連邦政府の行政機関を支援する情報システムのセキュリティ管理を規定したもの。		米国政府がサービスを提供するためのIDフェデレーション協定の一環として、サービス、手続き、慣行に関する年次監査。	アメリカ合衆国
FIPS-201	U.S. Federal Bridge Certification Authority (米国連邦ブリッジ認証局：FCBA)	PIV（個人ID認証）発行のための米国FBCAとの相互認証- 相互運用可能なICカードを米国政府と取引する組織に提供。		クレデンシャル・システム、物理的アクセス制御システム（PACS）、および PKI で使用される製品の年次認証を行い、GSA の承認製品リスト（APL）[9]への掲載を可能に。	アメリカ合衆国
DTAAP[11]の完全認定	EHNAC[12]			データ処理標準の遵守、およびセキュリティ・インフラストラクチャ、完全性、信頼される ID の要件への準拠を実証するための認定プログラム。	アメリカ合衆国
バミューダ公認サービスプロバイダー (CSP)	エネルギー・電気通信・電子商取引省	17799 (情報セキュリティ管理に関する実施規範), EESSI17[13] および認証局のための WebTrust		バミューダ公認証明書プロバイダーとしての認定を維持するための 2 年に 1 度の認証。DigiCertの子会社であるQuoVadisは、バミューダで唯一の公認CSP。	バーミューダ

[7]Federal Information Security Management Act(連邦情報セキュリティ管理法)
[8]Office of Management and Budget(行政管理予算局)
[9]National Institute of Standards(NIST)
[10]General Services Administration(一般調達局)
[11]Direct Trust Agent Accreditation Program
[12]電子医療ネットワーク認定委員会
[13]欧州電子署名標準化イニシアティブ

適用: ヨーロッパ

製品/スキーム	監督機関	トラストサービスの要件	認証機関／監査人	詳細	適用
ZertES 適格サービスプロバイダー	SAS[14]/BAKOM[15]	適格サービス・プロバイダー（CSP）およびタイムスタンプ機関に関するスイス法およびETSI[16] 規格	KPMG	適格証明書の要求事項への適合を確認するための年次監査。	スイス
eIDAS 準拠のためのオランダ ETSI 認証	Agentschap Telecom, オランダ	電子署名、Eシール、ウェブサイト認証のための適格証明書を発行するためのETSI EN 319 411-1 ETSI EN 319 411-2 v2.2.2[17] 規格 EU 規則 (EU) No 910/2014 (eIDAS)	BSI	EU域内における電子取引のトラストサービスに関する（eIDASとしても知られる）EU規則No.910/2014に基づくQTSPとしての認定のための年次監査。	オランダ - ただしEU全域で適用
PKIoverheid のためのトラストサービスプロバイダー（TSP）	PKIoverheidのためのLogius ポリシー管理局	Staat der Nederlanden ルートに対し電子署名、Eシール、ウェブサイト認証用の適格な証明書を認証発行するためのETSI EN 319 411-1, ETSI EN 319 411-2 v2.2.2 および PKIoverheid プログラム要件	BSI	オランダ政府のTSP認定を維持するための年次監査。	オランダ
オランダe-レコグニション／e-ヘルケニング	Logius オランダ政府（オペレーター） Agentschap Telecom（オランダ電気通信庁）（スーパーバイザー）	ISO 27001 (NL eHerkenning限定) ISO/ IEC 27001 ISMS要件への準拠	KIWA	組織を代表してオランダ政府サービスにアクセスするためのeHerkenning製品登録の提供。	オランダ
ベルギー適格トラストサービス・プロバイダー	ベルギー FPS 経済省 - 品質と安全	電子署名、Eシールのための適格証明書を発行に関わるETSI EN 319 411-1, ETSI EN 319 411-2 規格。 EU 規則 (EU) No 910/2014 (eIDAS)	BSI	ベルギーにおける個人の電子署名および法人のEシールの適格証明書プロバイダーとしての認定を維持するための年次監査。	ベルギー、EU全域でも適用
EUgridPMA[18] マネージドCA	IGTF[19] (APGridPMA[20] と TAGPMA[21]を含む)	IGTFの認証プロファイル		欧州の e-Science グリッド認証のためのトラストグリッドである EuroGridPMA のマネージド CAを運営するための認定。	ヨーロッパ

[14]Swiss Accreditation Service（スイス認定サービス）
[15]Bundesamt für Kommunikation
[16]European Telecommunications Standards Institute（欧州電気通信基準協会）
[18]European Policy Management Authority for Grid Authentication（グリッド認証のための欧州ポリシー管理機関）

適用: アジア太平洋

製品/スキーム	監督機関	トラストサービスの要件	認証機関／監査人	詳細	適用
ISAE[22] 3402	IAASB/IFAC[23]	ISAE 3402	BDO Sanyu	サービス組織の内部統制に関する年次監査	日本（DigiCert One）
特定認証業務向け監査		電子署名法	BDO Sanyu	PKIを運用するための電子署名法に準拠した監査	日本（PKI7）
ISO/IEC 27001		ISO/IEC 27001 ISMS認証（旧称：BS7799-2）への準拠	JICQA	日本データセンターにおける情報およびデータの安全な管理・保管状況を評価するための年次監査。	日本（DigiCert One）
Gatekeeper 認証	Digital Transformation Agency (DTA)	オーストラリア政府の保護セキュリティポリシーフレームワーク（PSPF）とオーストラリア政府および情報セキュリティマニュアル（ISM）	CyberCX	保護的セキュリティ・ガバナンス、人的セキュリティ、情報セキュリティ、物理的セキュリティを対象とする年次監査。	オーストラリア

業界データプライバシー規制の遵守

デジサート は、一般データ保護規則 (GDPR) およびカリフォルニア州消費者プライバシー法 (CCPA) を含む、適用されるプライバシー規制を遵守しています。その他の情報については、https://www.digicert.com/digicert- privacy-policy/ をご覧ください。

[17]証明書を発行するトラスト・サービス・プロバイダのポリシーとセキュリティ要件; Part 1: 一般要件。証明書を発行するトラストサービスプロバイダのポリシー及びセキュリティ要件; Part 2: EU 適格証明書を発行するトラストサービスプロバイダの要件。これらの TSP コンポーネント・サービスは、EU 規則 910/2014(eIDAS) に規定される以下の適格なトラスト・ サービスに対して提供される。
- QCP-n, QCP-n-qscd ポリシーに従った電子署名用適格証明書（適格トラストサービス）の発行
- QCP-l, QCP-l-qscd ポリシーに遵守したEシール用適格証明書（適格トラストサービス）の発行
- QCPw, QCP-w-psd2に遵守したウェブサイト認証用適格証明書（適格トラストサービス）の発行

[22]保証業務に関する国際基準

[23]国際監査・保証基準審議会／国際会計士連盟

DigiCert ONEの主な利点:

統合PKI管理

DigiCert ONEにより、顧客は企業ポリシーの遵守を徹底し、管理を合理化することができます。

TLS/SSL、エンタープライズPKI、コードサイニング、ドキュメントサイニング、IoTを含んだ統合PKIワークフローを1つのプラットフォームで実現します。

拡張性

コンテナ化されたアーキテクチャで構成されたDigiCert ONEは、大規模なビジネス向けの実装や成長による拡大ニーズをサポートできる高い拡張性を備えています。

実装の柔軟性

顧客は、クラウド（パブリックまたはプライベート）、オンプレミス、ハイブリッド構成など、データポリシーやインフラ要件に応じ柔軟な形態でDigiCert ONEソリューションを導入できます。

迅速な価値実現

DigiCert ONE を使用することで、インフラストラクチャのセットアップと管理を自動化し、CA/ ICA を迅速に作成することができます。

詳細については、弊社のウェブサイト<https://www.digicert.com/jp>のフォームよりお問い合わせください。