現実世界における
デジタルトラスト

digicert®

目次

アラスカの辺境から宇宙の果てまで

2013 年夏のある雨の日、小型の水上飛行機がアラスカのピーターズバーグ近くにある山の上で低空飛行中に失速しました。乗客は 6 名で、Le Conte（ルコンテ）氷河の観光ツアーに向かっていました。Horn Cliffs（ホーン・クリフス）に沿って上昇しようとした際に、パイロットの判断ミスから飛行機のコントロールを失い、きりもみしながら落下し、巨大な常緑樹に激突しました。

墜落事故の生存者は、負傷したまま急斜面に取り残され、自力で山を下りることは不可能に思われました。ほんの数時間で夜になります。6 月とはいえ、アラスカの夜は凍えるほどの寒さで、道路もありません。墜落機から全員を救出し、無事に連れ帰ることができるのは航空救助隊だけでしたが、そのような辺鄙な土地には携帯電話もなく、電波もほとんど届きませんでした。

しかし幸いにも、飛行機は上空 500 マイル（約 800 キロメートル）の軌道を周回するイリジウム衛星と接続しており、飛行機の緊急ビーコン信号を受信した衛星が、保護されたデジタル信号を使用して、遭難信号と場所を救助隊に送信しました。単なる GPS または無線遭難信号とは異なり、イリジウム対応機器は、飛行機が離陸してから墜落する瞬間までの動きを追跡し、フライト全工程のリアルタイムの航跡を把握していました。これは、66 のイリジウム衛星がそれぞれ衛星間および端末と通信を行うことで可能になります。イリジウム衛星ネットワークでは、南極大陸からアラスカまで、どこからでも、いつでも応答機器を見ることができ、通信を確保することができます。

飛行機が墜落した正確な場所を知ることで、米国沿岸警備隊は、数時間で事故現場に到着し、すべての生存者をヘリコプターで空から救助しました。

生存者を墜落機から安全に引き上げ、病院に搬送した後、Alaska Public Media が沿岸警備隊の報道官、Grant DeVuyst 氏にインタビューしました。彼は、緊急信号デバイスについて次のように述べています。「それは、事故があったことを知る唯一の手段であり、実際に現場にたどり着き、救出するための唯一の手段でもありました。」

デジタル・インタラクションは、買い物やEメール、アプリケーションのように、コンピュータやスマートフォン上でなされるものだと考えられる傾向にあります。しかし今日の世界では、デジタルとリアルの境界線は不明瞭になりつつあります。あらゆるものが接続され、この地上の膨大な量のデータや無数のデバイスのモニタや活用を可能にしています。

このような緊急事態では、生命が危険にさらされている場合、パイロットはイリジウム衛星ネットワークがフライトを追跡し、遭難信号を傍受して、救助隊に伝えることを知っている必要があります。ウェブサイトのトラフィックやEメールによる通信、一般的な意味での通信やデータの暗号化以上の必要性がここにあります。信号が確実に接続され、世界中で通信でき、現実で直ちに救出活動を行うという最も切迫した事態で機能する必要があります。イリジウム衛星がデジタルトラストの上に構築される理由はそこにあります。

「デジタルトラストは、海底から宇宙の果てまで、接続されたあらゆるものの セキュリティの 要となります。」

Brian Trzupek
デジサート製品担当上級副社長

リアルはデジタルであり、デジタルはリアル

今日では、あらゆるものが接続されています。リモートワークの職場から冷蔵庫まで、私たちが使用し関わるものは他のあらゆるものと繋がっています。端末はインターネット、インターネットはモバイルアプリと言っても過言ではありません。車にはコンピュータが搭載されており、医者の診察もバーチャルで済ますことができます。娯楽にはストリーミングが欠かせません。つまり、デジタルとリアルを区別する境界線はもはや存在しないのです。

接続されていることが当たり前の世界では、信頼はデジタルコミュニケーションを成り立たせる基礎となります。システムやデバイス、ユーザーとの対話は様々な形をとり、現実世界とバーチャルな空間に同時に存在し、ますます複雑化するグローバルネットワークを織りなします。従来のデジタルセキュリティも今なお重要ですが、暗号化するだけでは不十分です。このコネクテッドな世界を機能させ、通信を行うためには、テクノロジーや基準や実施手段を、デジタルトラストの包括的なシステムに内包することのできる、より柔軟で信頼性の高いアーキテクチャが必要です。

デジタルトラストとは何ですか？

デジタルトラストとは、個人や政府、企業や業界団体がデジタルの世界と信頼を確立するフレームワークであり、ソフトウェアであり、また営みでもあります。デジタルトラストは、接続された現状に対するニーズに応え、脅威に備え、デジタルテクノロジーの成長と進化を予測するうえで欠かせないものです。それを実現すべく、デジタルトラストは 4 つの柱に支えられています。

標準化団体

デジタルトラストに対するプロトコルやテクノロジー、およびアイデンティティの要件を定義する専門家や組織。例えば、CA/B フォーラムは SSL/TLS サーバ証明書の基準や、Web 全体のアイデンティティや暗号化の一般的なフレームワークを定義します。

コンプライアンスとオペレーション

コンプライアンスは、運営組織が定めた厳格な基準に従って業務が行われていることを検証する一連のポリシーと継続的な監査です。オペレーションは、データセンターを持ち、OCSP などのプロトコルを通じて証明書のステータスを検証します。

証明書ライフサイクル管理

ソフトウェアによって組織におけるパブリック / プライベートな信頼に必要な電子証明書のライフサイクル全体の一元化、可視化、管理を実現します。

あらゆるエコシステムにわたるデリバリー

複雑なサプライチェーンの中にまで、あるいはデバイスのライフサイクル全体へ、コンテンツコミュニティのデジタル著作権の証明へ、そしてオブジェクトがつながるその他の領域へ、信頼を拡大します。

現実世界におけるリアルトラスト

接続された二点間で信頼を確立するという考えは、デジタル通信と同時に発生しました。ところが、テクノロジーと理想との間に乖離が生じることもたびたびありました。信頼という概念の原理は、調和したハードウェアとソフトウェアのソリューションを欠いていたのです（逆もまた同様です）。真のデジタルトラストには、コンセプトとプロセス、ツールがいずれも重要です。デジタルテクノロジーと信頼という理想が価値を生み、大きな影響をもたらします。

テクノロジーや基準、実施手段を、デジタルトラストのシステムに内包する設計が必要です。

第 2 章

信頼の証明

ソリューションを構築するエンジニアやセキュリティの専門家でさえ、人々がデジタルトラストを使用する創造的な方法に驚かされることがよくあります。一見異種の技術や無関係な業界が織りなす糸のように、デジタルトラストは私たちが現実に通信し、移動し、仕事をするときの中心にあります。

航空

円滑な離陸、安全な着陸

複雑なエコシステムを使用している業界では、ネットワーク化している部品が多く、デバイスの能力に制限があり、またデバイスタイプ間の差異があるので、適応性と信頼性を備えたセキュリティソリューションが必要です。飛行機の場合、これらすべての要因が関与しますが、データの機密性も重要です。致命的な改ざんを回避するために、デバイス自体を保護するのと同時に、地上と飛行機の間で通信される情報も保護する必要があります。

デジタルトラストソリューションによりこれらのデバイスとそこで通信される情報を保護することで、パイロットと管制塔は安全かつ安心して様々な情報を収集、通信、使用することができ、飛行機や空港を問わず安全な離着陸が保証されます。AeroMACS を使用した場合、米国の小規模な空港でも、オーストラリアの大空港と同様に確実に機能します。

実装：世界的規模

デジサートのソリューションは、航空通信の基準であり、近いうちに世界中のすべての空港で使用されることになる AeroMACS ネットワークを保護します。

主なニーズ：認証

上空には常に数千の航空機が飛行している中で、空港、航空会社、およびパイロットは、毎日数百万人に対して安全で時間通りの旅行を保証するために AeroMACS に頼っています。

**2016 年以降、重要な情報は
デジタルトラストで保護された
飛行機の IoT センサーに
よって、世界中の管制塔と
飛行機に送られています。**

サプライチェーン

あらゆるものを特定

海を越えて大陸間である港から別の港へと輸送されている数百万の輸送用コンテナの 1 つがどこにあるか特定するとします。今度は 1 つの輸送用コンテナの場所をデータベースと貨物記録を使用して特定してみます。

国際的なサプライチェーンは複雑な時計のようなもので、機械を機能させるには、個々の歯、バネ、ホイールが適切な場所にあり、意図したとおりに動く必要があります。出荷の遅延は輸送網全体を減速させます。貨物の紛失は輸送網を崩壊させ、資材と利益の両方を失うことになり、企業に損害を与えます。

デジタルの見通し

毎年 110 億トン以上の商品が船で輸送されます。今日も、世界中に 5 万隻以上のコンテナ船が存在しています。海洋交易の規模は巨大であり、活動的でもあります。動きは一定で、貨物船は星空の地図のように地球上に点在しています。海上に多くの船が存在しているということは、さらに多くのコンテナが存在していることになります。これらのコンテナの位置を個々にリアルタイムで安全に特定して追跡することは大仕事です。

この規模で輸送する場合の課題は、資産が追跡されるフィールド内のデバイスやクラウドに対して、相互認証することです。万が一侵害されれば、海運会社はコンテ

ナの位置を見失ったり、コンテナについて間違った情報が会社に送信される恐れがあります。有効な対策としては、セキュリティソリューションでデバイスだけでなく、送信される情報も保護する必要があります。さらに、一度に数万のデバイスを確実に保護できるスケーラビリティも必要です。

世界中のどの航路のどこにいても

デジタルトラストを使用すると、輸送用コンテナは出港から仕向港までの全航路を通して、貨物の数に関わらず、世界中のどこにあっても確実に追跡されます。これにより盗難や紛失のリスクが低下し、港から港までの商品の効率的な輸送が保証されます。

実装：世界的規模

グローバルなサプライチェーンの中では、接続された輸送用コンテナが地球上のどこにでも商品や資材を輸送します。

主なニーズ：認証

単なる追跡ではなく、デジサートのソリューションはリアルタイムで安全な認証を実現し、企業が個々の輸送用コンテナに取り付けられたデバイスの位置を特定し確認できるようにします。

デジタルトラストを使用すると、輸送用コンテナは全航路を通して、確実に追跡されます。

世界中の勤務地

いつでも、どこでも、誰でも

企業の規模を管理することは、企業が生産するものを管理するのと同じくらい大きな課題になることがあります。例えば、世界中の様々なオフィスで様々な役割で働いているだけでなく、異なる OS やアプリケーション（その多くは BYOD）を使用し、異なるデバイスで作業している従業員を企業はどのように保護すればよいでしょう?

IBM にとって、これは単なる課題演習ではありません。これは現実の問題であり、新型コロナウイルス感染症により、多くの企業がリモートワークを導入せざるを得なくなったずっと以前から解決する必要がありました。

すべて持ち込み可能

50 万人以上のユーザーを認証、特定し、保護する必要がありました。

ここでは、「フレキシブルとスケーラブル」という言葉は、単なる論理的な説明ではなく、実用的なデジタルトラストソリューションの現実的な機能である必要があります。しかし、従業員の数が課題であると同時に、それらの従業員が実行し、仕事に持ち込むデバイスやアプリケーションの種類の数も、それ以上とは言わないまでも、同様の課題を突きつけてきます。会社所有のラップトップ。個人のスマートフォン。古い iPad。従業員、ベンダー、請負業者にとって、最も働きやすいデバイスを使用させる柔軟性を提供する一方で、ネットワークに脆弱性を持ち込みたくない場合は、適応性がありながらも、堅牢なセキュリティソリューションが必要です。

この場合は、フレキシブルであると同時にスケーラブルでもある必要があります。デジタルトラストには、こうした基本的な属性が備わっています。つまり、IBM はデジタルトラストソリューションを使用して何台でも、その所有者や実行している内容を問わず、数百、数千の従業員に関して、彼らがどこにいても複数のデバイスの認証を同時に行うことができたのです。50 万人もの従業員が完全にシームレスにつながります。

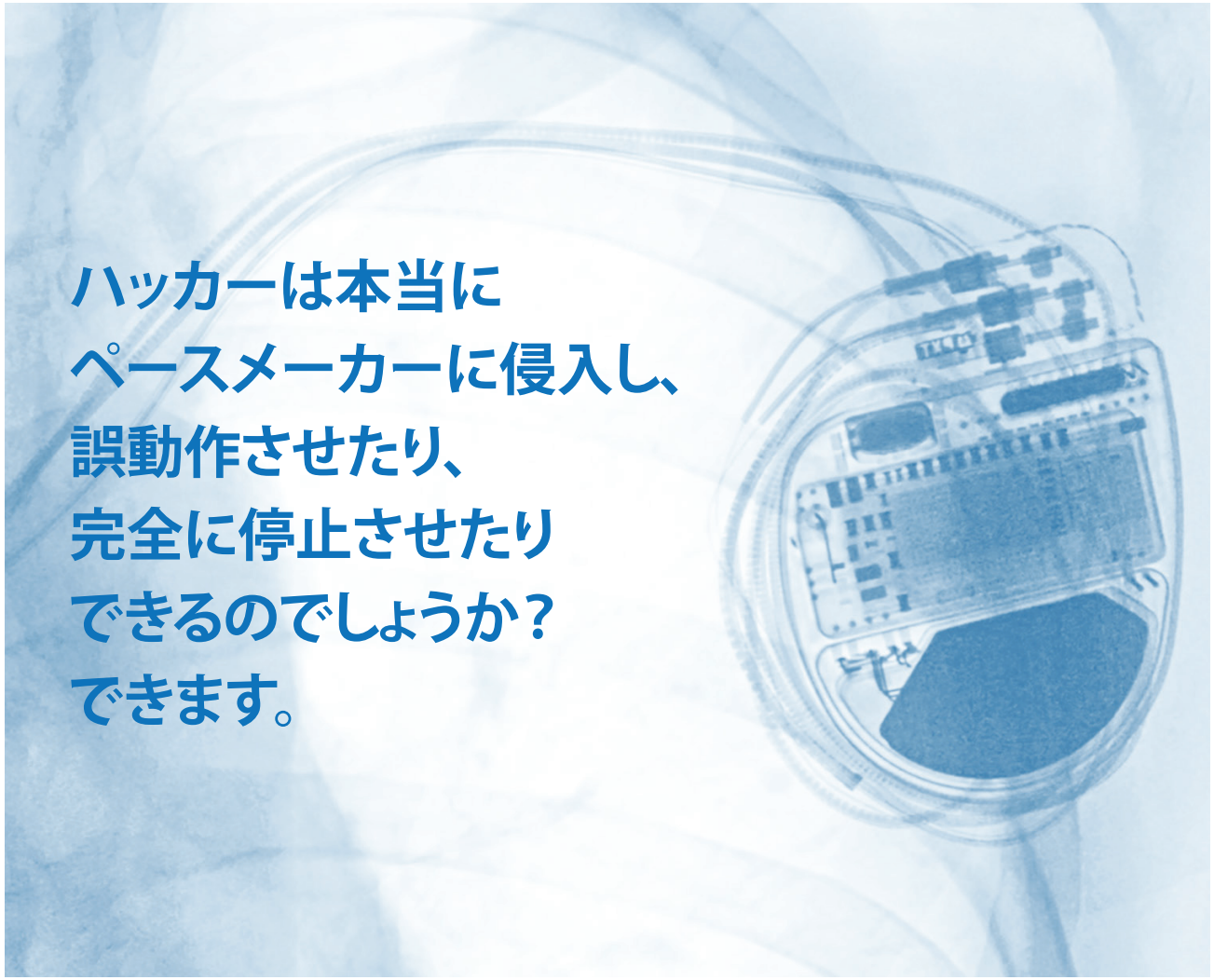
実装：世界的規模

世界中に存在する数千のオフィスでは、ハードウェアおよびソフトウェアの長年にわたる世界的なリーダーとしてビジネスを行っています。

主なニーズ：フレキシブルとスケーラブル

重要な業務をオンラインで行う際、PKI は世界中の 50 万人の従業員を認証、保護、特定するためのソリューションを提供します。

システムが接続された
環境の従業員、ベンダー、
請負業者に必要なのは、
堅牢で適応力のある
セキュリティです。



医療

命がかかっているときの信頼性

ほとんどの人にとって、デジタルデバイスは便利をもたらすものです。Bluetooth 接続があれば、現在の庭先の温度と湿度を確認できます。キッチンの iPad とリビングのスマート TV を Wi-Fi で接続すれば、夕食をオーブンに入れている間、続きのエピソードを視聴できます。ネットワーク化は便利なものですが、不可欠なものとは限りません。ただ一部の人にとって、接続は生死の問題です。

数年前、メディカルエンジニアが新しい形のペースメーカーを発表しました。この特別なモデルは「スマート」でした。ペースメーカーを外部モニタと患者の電話アプリに Bluetooth で接続すると、心臓を動かしておくために必要な電気信号を送れるだけでなく、ペースメーカーがどのように機能しているかを患者と医師に伝えることができるのです。ペースメーカーが正常に機能しているか。バッテリーの残量はどのくらいか。これまで、このような診断や治療には、来院や、ときには手術が必要でした。今では、すべて自動的に継続してモニタ、記録、通信ができるようになりました。

接続されたペースメーカーは単に便利なだけではありません。数千人が生命の維持をこのデバイスに頼っています。しかし、他の接続と同様に、障害も考えられます。ペースメーカーを使用する人々にとっては、デジタルトラストの必要性は極めて重大であり、また切実なものです。

文字どおりの「死活問題」

2017年8月、少なくともIoTの世界に関わっていない人にとっては異常な見出しのニュースが報じられました。アメリカ食品医薬品局（FDA）がサイバーセキュリティに対する脅威から、多数のペースメーカーをリコールしたのです。インターネットハッキングのリスクに関する他の話のように、FDAは、特定のペースメーカーに「サイバーセキュリティを利用した侵入と悪用に対する脆弱性」が考えられると警告しました。それは、SF映画の筋書きのようにも思えるとんでもないものでした。ハッカーは本当にペースメーカーに侵入し、誤動作させたり、完全に停止させたりできるのでしょうか？できます。

医療機器メーカーが、病院用スマートベッドから持続血糖モニタまで、医療デバイスをネットワーク化し斬新で価値のある方法を発明したことで、患者の利便性が向上しました。それと同時に、接続されたデバイスによって収集された患者データの保護に関する懸念、さらには、デバイスの故障につながる侵入に関する懸念も高まりました。

実際に、ハッカーはペースメーカーでまさにこのような侵入ポイントを見つけました。メーカーは、ペースメーカーとベッドサイドモニタ間の通信を暗号化しましたが、モニタそのものは保護されていませんでした。ハッカーは、モニタにアクセスしてペースメーカーに繰り返しコマンドを送り、バッテリーを消耗させることができました。さらに悪いことに、患者にショックを与えるようにペースメーカーに指示することができました。デバイスだけでなく、患者の安全も守るための手段を探す中で、多くのメーカーがデジタルトラストソリューションに注目しました。

今日、簡単で安全な監視システムが守ってくれていることで、ペースメーカーが継続的に機能し潜在的な問題があれば警告されることを知って、何千という人が心の平安を享受しています。

近い将来、循環器検査の能力が向上すれば、より多くの患者とその医師に、より有用なデータと手術や来院が不要な緊急支援に関してより多くの選択肢が提供されます。医療機器はより小型化され、より高性能になりますが、患者のデータと生命を継続的に保護するセキュリティソリューションはデジタルトラストになるでしょう。

実装：複数の国々、世界的規模

何千もの病院や医療センター、数百万の人々が、異なるコンプライアンスと実施基準を越えてプロバイダーと患者が同様に使用します。

主なニーズ：信頼性

デバイスと患者データの完全性を守り、命がかかっているときに十分信頼できるセキュリティソリューション。

証明済みのテクノロジー

立証されているテクノロジーがないデジタルトラストは単なるスローガンに過ぎません。現実世界にデジタルトラストを実装するには、膨大で複雑な状況下で保護された接続を可能とするソフトウェアとシステムが必要です。どんなテクノロジーにもできることではありません。現実世界で信頼を機能させるためには、接続は証明されたセキュリティソフトウェアやプロトコルを基盤とする特定の資質を持っている必要があります。

安全な接続は、以下の３つの原則の上に成り立ちます。

アイデンティティ

個人、企業、マシン、ワークロード、コンテナ、サービスなど、接続するものはすべて、暗号的に一意なアイデンティティによって認証される必要があります。

データの完全性

オブジェクトの使用と伝送には、改ざん防止とともに、オブジェクトが改ざんされていないことを検証するツールも必要です。

暗号化

伝送されるデータは保護される必要があります。

現実世界で信頼を機能させるためには、接続は証明された安全なソフトウェアやプロトコルを基盤とする必要があります。

基盤となる PKI

公開鍵基盤は、ウェブサイトの保護に数十年にわたる実績があります。コネクテッドな世界が長い年月をかけて進化するにつれ、デジタルセキュリティの専門家はウェブサイトの暗号化に使用されている証明されたテクノロジーが、データを認証しながらアイデンティティを検証することができることに気がつきました。これらの電子証明書はネットワークから E メールへ、コードから文書へ、そしてユーザーやデバイスへ、ほぼあらゆるデジタルオブジェクトに発行することができます。その本質から、PKI はデジタル通信の暗号化、データの完全性、アイデンティティをもたらします。PKI がデジタルトラストの基本的な要素であり、あらゆる課題に対応するのはまさにそのためです。

柔軟性

今日のエコシステムでは、担当者はウェブサイトに加えてアプリケーションも保護したり、電子書類に安全な署名をしながら従業員のスマートフォンを認証する必要があります。ある企業では、製造ラインの自動化ロボット用のソリューションを必要とする一方で、別の企業は顧客のクレジットカード番号を保護するソリューションを必要としています。1 つの手段としては機能しても、他では機能しない、またはある時点には機能しても翌日は機能しないというソリューションは、セキュリティを管理する IT チームの負担になるだけでなく、企業を危険にさらします。

他のセキュリティソリューションとは異なり、PKI は信じられないほど柔軟です。PKI は、非対称鍵ペアを利用し、セキュリティプロセスで検証と同じくらい簡単に暗号化を行えるため、様々な環境に導入して、幅広い接続を保護することができます。PKI ソリューションは縮小も拡大も可能で、クラウド、オンプレミス、ハイブリッドで稼働し、今日は Web と E メール、明日は BYOD と IoT を保護するということも可能です。1 つで複数のセキュリティニーズに対応できるソリューションです。

パブリック、プライベート両方の信頼

単なる暗号化だけでなく、PKI は署名プロセスを使用して ID と鍵を結びつけます。署名はルートより発行されるため、そのルートの公開鍵を持っていれば、誰でも PKI 証明書にバインドされた署名が有効で信頼できるかが分かります。

パブリックルートの場合、Chrome や Firefox などのウェブブラウザや Microsoft Windows や Apple MacOS などのオペレーティングシステムによって保護された信頼できるストアより配信されます。プライベートルートの場合は、企業が内部的に使用する任意のシステムまたは小規模な企業グループ内でのみ信頼されます。暗号化はどちらのケースでも同様に行われますが、パブリックとプライベートの両方のオプションに対応できることが、PKI の汎用性を高めています。

この柔軟性により、PKI はパブリックとプライベートの信頼性のギャップを埋めます。多くの国の政府向けのプライベート暗号化および ID ソリューションとして信頼できるだけでなく、同様にコンシューマー向けの IoT デバイスのパブリックソリューションとしても信頼できるほど十分に強力で安全です。

デジタルトラストを実践で活用

デジタルトラストで最も重要なことは見過ごされやすい傾向にあります。デジタルは、もはや単にデジタルという意味ではないのです。デジタルトラストの核心は、ビジネスの基本や合意、社会契約、ささやかな人々の対話など、数千年前から見出せるものです。その空間が物理的かバーチャルに関わらず、その対話や通信が認証され、安全であり、交換する情報が合理的で不変であることを確認することが重要なのです。

デジタルトラストは単に高尚な考えでもなければ、セキュリティソフトウェアでもありません。デジタルトラストとは、あらゆるものやあらゆる人と繋がり、通信を行うときの信頼です。その意味では、デジタルトラストで重要なことは、それが何かということではなく、それで何をするかということなのです。

デジサートについて

米デジサート・インク（本社：ユタ州リーハイ、非公開企業）は、インターネット上で人と企業と政府とコンソーシアムが電子的な信頼でつながることができるようにする、デジタルトラストのリーディング・プロバイダーです。

DigiCert® ONE は、企業向けのデジタルにおける信頼のためのプラットフォーム OS であり、Web サイト、企業アクセス、通信、ソフトウェア、ID、コンテンツおよびデバイスを保護し、デジタルトラストの幅広い認証ニーズに対する可視化と一元管理を提供します。デジサートは、受賞歴のあるソフトウェアと、標準、サポート、および運用における業界のリーダーシップとを結び付ける存在であり、信頼を実践で活用する世界中の大手企業から選ばれるプロバイダーです。

デジタルトラストを実践で活用してみませんか？
詳細は sales@digicert.com までお問い合わせください。