IDC

デジタルトラスト：デジタルフリーダムの基盤

RESEARCH BY:

Jennifer Glenn
Research Director,
Security and Trust Group, IDC

2022年11月 | Doc. #US49795922

目次

タイトルまたはページ番号をクリックすると該当セクションへ移動します。

デジタルトラストの定義

デジタル世界の到来で、膨大な量の情報やツールが簡単に利用できるようになった。デバイスやアプリケーションがビジネスデータとユーザーをつなぎ、コラボレーションの改善、業務の効率化、イノベーションの拡大を実現している。個人向けのデバイスやプログラムでは、家計管理や健康データのモニタリングから家電製品の操作やオンラインショッピングまで、あらゆるモノに関する個人情報を統合している。すべてのツールはインターネットを介した接続や継続的なデータ通信のインフラストラクチャに依存している。仕事や日常生活においてこれらのツールは重要であり、依存していることを考えると、これらの接続が中断、終了、変更された場合には、必ず問題が発生する。そのため、デジタルインフラストラクチャを構成するエンティティやデータを高度に保護し、検証しなくてはならない。したがって、デジタルトラストが必要になるのである。

デジタルトラストは、ユーザーが恐れることなくデジタル世界に関われるようなテクノロジー、プロセス、ポリシーを戦略的に導入することで達成できる。それは、世界が拠り所とするデジタル製品やサービスが本物で、安全であるため、安心して使えるというある程度の信頼や保証である。そして、悪意ある者による侵害に怯えることなくデジタル世界と繋がり、仕事をし、余暇を楽しむことができる自由である。

デジタルトラストを実現する構成要素の理解

デジタルトラストは重要であるにもかかわらず、その仕組みは機能してあたりまえと思われがちである。一般的な消費者やビジネスユーザーは、オンライン作業の際に情報やサービスがどのように届けられるかというプロセスを通常は考えない（ただし、目的の情報やサービスが損なわれたり利用できなかったりすると、ブランドの信頼が損なわれる可能性はある）。デジタル基盤の仕組みを作成／管理してきたのは、従来、PKI（Public Key Infrastructure：公開鍵基盤）などの主要テクノロジーの技術的複雑さを理解することに専念してきたIT専門家であった。

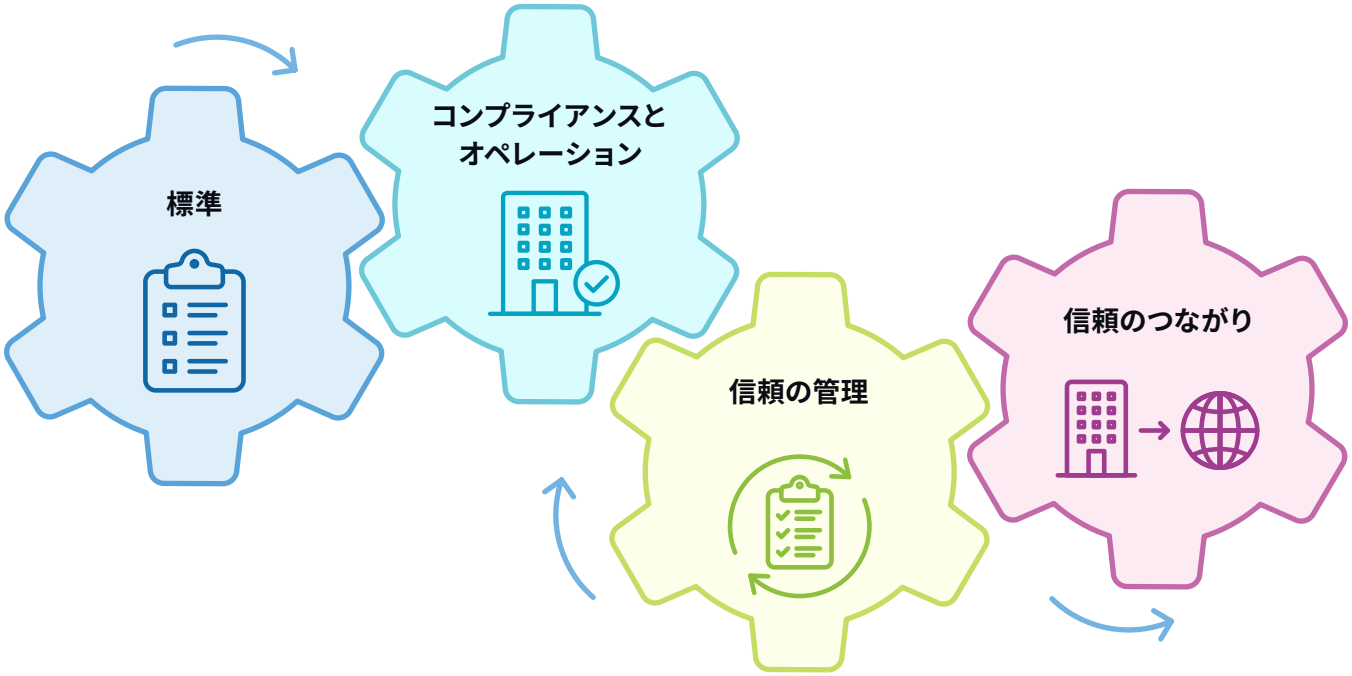
PKIは、ユーザーやデバイス間で暗号鍵情報を交換するために使用されるインフラストラクチャ（規則、プロセス、テクノロジーを含む）で構成されている。これらの鍵は、データの保存時、インターネット上のさまざまな場所への送信時、アプリケーションの使用時に、データを暗号化／復号するために必要となる。

現在、この鍵交換は一様にデジタル証明書を用いて行われる。デジタル証明書は、少なくとも鍵と署名で構成される。また、多くの証明書には、鍵を管理するエンティティを正確に特定するための識別情報も含まれている。PKIの利用は、安全なオンライン通信の促進や署名の完全性の確認に不可欠であり、デジタルトラストを構築するための基盤となっている。

すべての戦略的構想は、明確な方向性と最終目標、測定可能な目標、強力な管理、堅実なサポートから恩恵を受ける。デジタルトラストも例外ではない。**Figure 1**に示す4つの構成要素は、デジタルトラストを無事に達成するための構造と定義を示している。

FIGURE 1

デジタルトラストの4つの構成要素



Source: IDC, 2022

標準

どのようなシステムであっても、参加者の相互運用の方法や、作業プロジェクトを作成するための最小限の要件に関するフレームワークを、それぞれに対応する標準で定義する。Certification Authority (CA)/Browser Forum、Matter、SAE International、Internet Engineering Task Force (IETF)、European Telecommunications Standards Institute (ETSI)、Internet Corporation for Assigned Names and Numbers (ICANN) など、デジタル証明書が中心的役割を果たすさまざまなユースケースのデジタルトラストに関連する標準化団体が数多く存在する。標準要件の変更や調整を常に把握しておくことは課題のひとつではあるが、注目を集める攻撃やデータ要件によって、どのようなデータを保護する必要があるのか、どのように使用できるのかについて、消費者の意識はますます高まっている。このことが、業界の管理機関にとって標準要件の更新や変更を行う原動力となるのである。

デジタル証明書の場合、CA/Browser Forumなどの業界団体が、認証局であるCAが証明書を発行できる時期、その証明書の内容、証明書を失効させる時期について明確なガイドラインを提供している。PKIに関する標準は、証明書のユースケースや保護される情報の重要性によって異なる。

ビジネスにおけるデジタルトラストの強固な仕組みを構築するには、これらの標準要件や変更点を把握することが重要である。標準の把握と管理を独自に行う組織もあるが、ほとんどはこれらの把握をCAに依存している。誰が責任を負うかにかかわらず、賢明な組織は、証明書の検証基準に関する変更の把握および管理のプロセスだけでなく、最新のガイドラインを常に把握しておくための監査を行う明確なプロセスも設けるべきである。

コンプライアンスとオペレーション

標準を知り、理解することもそうだが、各参加者がこれらの標準を遵守するよう規制するだけでも取り組みのひとつになり得る。コンプライアンスには2種類の測定方法がある。まず、標準化団体によって設定された標準を組織がどの程度満たしているかを測定し、実証する方法を提供する。ビジネスオペレーションの観点から見ると、これはさまざまな標準を満たすために必要なもののチェックリストのように見えるかもしれない。これが2つ目の測定である、内部測定につながる。たとえば、社内にサーバーやデバイスの証明書を購入するチームが複数いる場合、こうしたチェックリストによって、組織内の全員が共通の理解を持てるようになる。デジタルトラストとは、全社的な取り組みである、またはそうあるべきであり、このような一貫性は、各部署がこれらを成功するための目標に照らして測定するための重要な方法である。

さらに、その組織と連携するサプライヤーやその組織の製品やサービスに依存する消費者にとっては、その組織が業界標準をどのように把握し遵守しているかを確かめることで、品質と信頼に対するその組織の責任の明確な証拠が得られる。

信頼の管理

業界標準の遵守に伴い、鍵、アイデンティティ、証明書など、複数のユースケースに渡って信頼の管理を統一する必要が発生する。複数のチームがさまざまな目的で証明書を購入することがあり、ビジネスにおけるコンプライアンスを十分に理解することで一貫性を持たせても、信頼を構成する各要素のライフサイクルが異なる場合がある。たとえば、TLS（Transport Layer Security）証明書の有効期限は最大398日であるが、3年ごとに鍵のローテーションを必要とするプログラムもある。コンプライアンス要件に抵触することを避け、セキュリティを最適化するために、信頼の各要素を管理する必要がある。信頼をうまく管理できないと、停止やインシデントにつながる可能性がある。証明書の有効期限切れによる1回の停止も問題だが、重要なシステムの停止が他のシステムに波及し、そのシステムに依存しているビジネスの他の分野に広範な問題を引き起こすかもしれない。

デジタル証明書の管理で最も大きな課題の1つは、可視化である。複数の部署が証明書（パブリックおよびプライベート）を購入する場合、組織が管理する証明書は数万枚に及ぶこともある。これらの証明書が何らかの中央管理システムを経由していない場合、どのシステムの証明書を更新する必要があるのか、あるいは、前述した証明書がコンプライアンス基準を満たしているのかを知ることはほぼ不可能になってしまう。加えて、流通している証明書の数がかなり多いため、管理が非常に困難である。したがって、可視化問題に取り組むことは、プロセスを自動化するための基準、または少なくとも正当化の理由となり得る。

デジタルトラストの実現を目指す組織にとって、証明書の一元管理は不可欠である。ある大手テクノロジーベンダーは次のように述べている。「*当社は事業全体のすべての証明書を一元管理する方法を必要としていました。それは、次の有効期限を把握するだけでなく、更新プロセスを自動化できるようにするためでもあります。どちらも、企業にとって致命的となるサービス停止のリスクを減らすのに役立ちます*」

信頼のつながり

デジタルトラストの仕組みを構築するために組織が必要とする最後の構成要素は、このレベルのセキュリティの責任および証明を、自社のブランド名とソフトウェアを持ちながらも自社の管理外で動作する、増え続ける接続デバイスにまで拡大することである。これには、ホームオートメーションやウェアラブルな健康管理デバイスなどが含まれる。

このタイプのデバイスには運用上の課題が数多く存在する。これまで説明してきた他の構成要素と同様に、IoT（Internet of Things：モノのインターネット）デバイスを最適に動作させるために必要な証明書の数を把握し続けることに忙殺される可能性がある。各デバイスはそれぞれ異なる証明書を持っている可能性があるが、証明書の認証はデバイスに接続するWebアプリケーション、クラウドサービス、ゲートウェイでも行われる。デバイスはこれらの接続に依存しているため、機器のセキュリティと送信データの保護を確保するために、すべて適切に認証されなければならない。最後に、デバイスはダウンタイムなしに、迅速に更新される方法が必要である。そのためには、デバイスと組織の間の安全な通信が必要である。

これらのデバイスの目的を考えると、信頼性とセキュリティの確保とコードの完全性の維持がかなり重要となる。前述の分野のいずれかを誤ると、サービスの停止につながる可能性がある。ひいては、ブランドの評判を落とすだけでなく、法的措置につながる可能性もある。

これらの分野はそれぞれ、デジタルトラストの仕組みの重要な構成要素を示している。組織がこれらの分野の1つ、または複数で欠陥があれば、デジタルトラストは不完全となってしまうのである。

デジタルトラストを戦略的構想にするベネフィット

過去10年間で、サイバーセキュリティについての見方は、実用的なものから戦略的なものへと変化している。これは、ランサムウェア攻撃やデータ漏洩が大々的に報道されたことが主に起因すると考えられる。また、データプライバシーやコンプライアンスに関する規制も、この変化の一因であり、セキュリティチームの活動にスポットライトが当てられた。そのため、暗号化、鍵の管理、証明書など、デジタルトラストに不可欠な基礎的要素の大部分は、IT部門の小人数チームに委ねられている。

長年に渡り、PKI管理者と暗号化運用チームは、ひっそりとデジタル世界が崩壊しないようつなぎとめてきた。彼らの仕事とその成功は、気づかれていないか、セキュリティ機能がその仕事をしていると誤解されていることが多い。セキュリティがもっと経営者の目に留まるようになれば、この状況は変わる可能性があるし、変わるべきである。

デジタルトラストの導入を成功させるには、IT部門の少数の管理者グループだけに委ねるべきではない。あらゆるサイバーセキュリティの取り組みと同様に、デジタルトラストは、ビジネス全体の責任である。デジタルトラストの実現を中心とした望ましいビジネス成果に焦点を再設定することで、組織はビジネス全体を奮い立たせ、次のようなベネフィットを実現できる可能性を示唆する。

- **顧客満足度とエンゲージメントの向上：**IDCが2022年6月に実施した「Future Enterprise Resiliency and Spending Survey」によると、顧客満足度と業務効率は、世界中のビジネスの優先順位で上位にランクされている。これは、顧客が必要とするデバイス、アプリケーション、サービスが利用可能で、適切に機能し、理想的なエクスペリエンスを提供することを意味する。
- **業務効率の向上：**デジタルトラストへの取り組みによって、組織は運営の効率化を図れる。証明書管理を一元化することで、自動化の基盤が構築され、証明書の状況の可視性が向上する。この2つの活動は、ビジネスにおけるシステムの継続的かつ効率的な運用に貢献している。
- **全体的なセキュリティ体勢の強化：**デジタルトラストのための各構成要素の導入とは、従業員間で使用される通信ツール、顧客向けの情報を表示するサーバー、世の中に出回るIoTデバイスなど、必要とされるあらゆる場所に一貫したセキュリティ管理を取り入れることを意味する。

デジタルトラストへの取り組みに対するDigiCertの検討

このデジタルトラストの仕組みにおける個々の構成要素に取り組む組織を支援するベンダーやコンサルタントは数多く存在する。適切なパートナーを選択することは非常に重要である。

2003年に設立されたDigiCertは、デジタルトラストのグローバルプロバイダーであり、企業と消費者の両方がデジタルフットプリントの安全性を確信できるような包括的なソリューションを提供している。DigiCertは、アイデンティティ、認証、暗号化、完全性という基盤となる柱を提供している。同社は、標準、コンプライアンスとオペレーション、信頼の管理、デジタルエコシステムへの信頼性の拡大といった、デジタルトラストの構成要素を提供している。業界のリーダーであるDigiCertは、CA/Browser Forum、Matter、SAE、IETF、NISTにおけるリーダシップを含め、デジタルトラストのための世界標準の開発を支援している。DigiCertは、数多くの業界をサポートし、複数のベンダーと協力しながら、デジタルトラストの標準の作成と導入を支援している。同社は世界の20か所にオフィスを構え、コンプライアンス、アップタイム、信頼性を確保するためグローバルに分散したデータセンターを展開している。

DigiCert ONEプラットフォームは、地域やローカルのニーズに対応しつつ統一された信頼の管理を提供する。DigiCert ONEとそのManagerモジュールは、組織が証明書の状況を把握するために信頼の管理を統一できるように支援し、完全なレポート機能、発見と自動化、パートナーツールとの統合の深化を特徴としている。また、DigiCert ONEは、ソフトウェアサプライチェーン、接続デバイスエコシステム、文書および電子署名にも信頼を広げ、オンプレミス、クラウド、DigiCertホスティング、ハイブリッド展開モデルを通じて、あらゆる環境で利用できる。最近Mocanaを買収したDigiCertは、製造の前段階から製造中、そして現場でのデバイスのエンドツーエンドのライフサイクルセキュリティを追加した。

課題と機会

PKIのような従来の「技術的」な概念に基づいてビジネスの成果や優先順位を再考しようとすると、課題に直面する。多くのビジネスリーダーにとって、PKIやデジタルトラストのその他の要素は、インターネット上でビジネスを行うためのコスト／プロセスの一部にすぎない。PKIはほとんどユーティリティのように考えられており、しかも理解する必要もなければ理解をしようとも思わない非常に技術的な部分であるため、壊れているように見えないのになぜ変えるのか、という*思考プロセスが蔓延*している。

セキュリティチームやPKI管理者にとって、これはPKIの価値を広く知らしめ、デジタルトラストの仕組みを構築する良い機会であり、デジタルトラストの仕組みにおける過失によって生じるかもしれないリスクや、このプロセスの効率性を見つける機会も示しているのである。

結論

デジタルトラストは、単にそれを可能にするテクノロジーというだけではない。組織がデジタルトラストの推進派になるためには、それを可能にする構造、プロセス、活動を理解し、積極的に実行する必要がある。これには、業界標準の変更の把握、各地域の規制要件の継続的な遵守、デジタルトラストテクノロジーのライフサイクルの管理、デジタルエコシステムへの信頼の拡大などが含まれる。規模に関わらず、多くの組織にとってこれは熟練したスタッフ、専念する時間、予算を必要とする重要な事業である。デジタルトラストの成果に尽力する組織は、先に説明したデジタルトラストの各構成要素を導入及び管理する能力を検討し、必要に応じてそれらのプロセスの1つまたは複数の管理を支援してくれるパートナーを探す必要がある。これは、特に経営幹部の地位にある人たちにおけるマインドセットの転換である。しかし、デジタルトラストに注力し、それをビジネスの戦略的必須事項とした企業にとって、信頼できるアップタイム、データ漏洩リスクの低減、ユーザーの信頼性の向上など、ベネフィットは顕著である。

アナリストについて

Jennifer Glenn
Research Director, Security and Trust Group, IDC

Jennifer Glennは、IDC Security and Trust Groupのリサーチディレクターで、情報およびデータセキュリティの実践の調査を担当している。メッセージングセキュリティ、機密データ管理、暗号化、トークン化、権限管理、鍵管理、証明書など幅広いテクノロジーを主に対象とする。この調査の一環として、顧客の信頼獲得やデジタルトランスフォーメーションといった企業の最上位の取り組みにおけるデータセキュリティの重要な役割を実証する予定である。

Jennifer Glennの詳細

スポンサーからのメッセージ

DigiCertは、世界中の主要な組織と提携し、実世界の成果を促進するデジタルトラストイニシアティブに取り組んでいます。

DigiCertがお客様の目標をどの様にサポートできるかについて、詳しくは、www.digicert.com/jp をご覧ください。

IDC Custom Solutions

本調査はIDC Custom Solutionsが発行したものです。ITおよび通信分野、消費者向けテクノロジー市場に関する調査・分析、アドバイザリーサービス、イベントを提供する世界大手のグローバル企業として、IDC Custom Solutionsグループはお客様がグローバル市場でプランニング、市場進出、販売、成功するための支援を行っています。当社は、実用的なマーケットインテリジェンスと、測定可能な結果をもたらす影響力のあるコンテンツマーケティングプログラムを構築します。

IDC @idc @idc idc.com