LEADERS

LAGGARDS

PKI

2024年 デジタルトラストの実態調査

COMPLIANCE

DIGITAL TRUST FOR THE REAL WORLD

IoT

OUTAGES

XX
SECURITY ALERT

BEST PRACTICES

digicert®

2024 年デジタルトラストの実態調査

2022 年、デジサートは「2022 年デジタルトラストの実態調査」を発表しました。デジタルトランスフォーメーションがあらゆる業界に広がる中、接続先のユーザーとデバイスが正当であり、安全に通信が行われることを確認するためにデジタルトラストが不可欠になっています。

IDC のリサーチディレクター、Jennifer Glenn 氏は、デジタルトラストを「つながった世界を保護するための基盤であり、顧客、従業員、パートナーがオンラインビジネスのプロセスやインタラクションが安全であるという信用を得たい組織にとって不可欠なもの」と定義しました。

デジサートは、デジタルトラストをお届けする世界有数のプロバイダーとして、個人と企業が、デジタル世界におけるそれぞれのフットプリントの安全性を信頼してオンラインで取引できるよう取り組んでいます。お客様のお役に立つため、デジサートではグローバルな組織がデジタルトラストをどのように認識し、デジタルトラストの確立、管理、拡大にどう取り組んでいるかを理解することに全力で取り組んでいます。

トラストの知見を活かす

最初の調査では、100% の企業がデジタルトラストは重要だと感じていることが分かりました。ほぼすべての企業（99%）が、顧客が自社への信頼を無くした場合、競合他社に乗り換える可能性があると考えていました。ほとんどの消費者も同意見であり、消費者の 3 分の 2（68%）がデジタルトラストは重要だと回答しました。

この最新の報告書では、前回の報告書でわかったことを深く掘り下げています。デジサートの 2024 年デジタルトラストの実態調査では、デジタルトラストの特定の役割とワークフローを詳しく調査し、企業の現在の状況を確認するとともに、企業がこれからもデジタルトラストの取り組みを最適化し続ける方法を考察します。

調査方法

2024 年デジタルトラストの実態調査は、ダラスに本社を置く Eleven Research によって 2023 年第 4 四半期に実施されました。調査は北米、EMEA（ヨーロッパ / 中東 / アフリカ地域）、APJ（日本を含むアジア太平洋）の中小～大企業までの上級意思決定者 300 人を対象に電話調査を実施しました。さらに APAC 版の調査では日本を含むそのうち 100 名のアジア、太平洋地域のデータを選択しその特徴をとらえました。

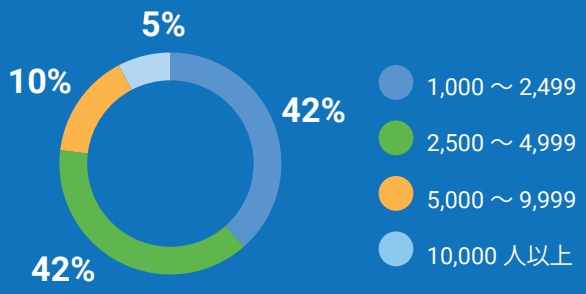
テクノロジー、製造業、金融サービスなど、さまざまな業界の方々に話を伺いました。企業規模としては従業員数 1,000 ～ 10,000 人超まで多岐に渡ります。

デジタルトラストの特定の取り組みをより深く理解するため、Eleven Research では以下の 4 種類のデジタルトラスト分野の責任者に焦点を当てました。

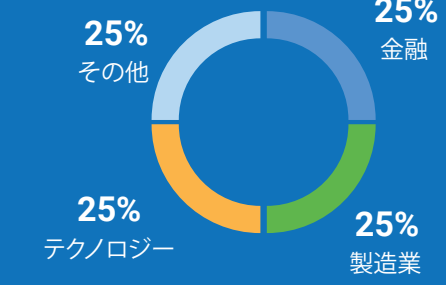
- エンタープライズ – コミュニケーションとデータの保護、そして従業員、アプリケーション、クラウドからのアクセスを保護する
- IoT とコネクテッドデバイス – 血糖値モニターなどのスマートデバイスやサービスを保護する
- ソフトウェア – ソフトウェアやアプリケーションの改ざんやサプライチェーン攻撃から保護する
- 電子署名 – 文書やコンテンツの真正性と完全性を保証する

地域

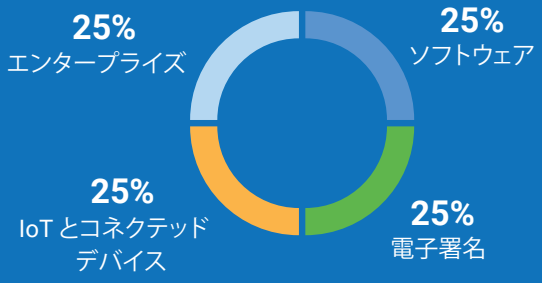
企業規模



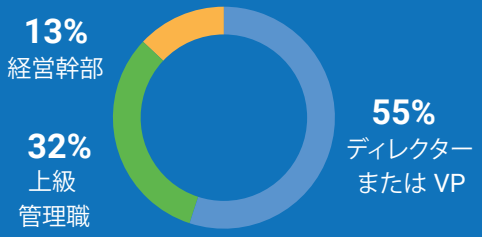
業種



ペルソナ



職位

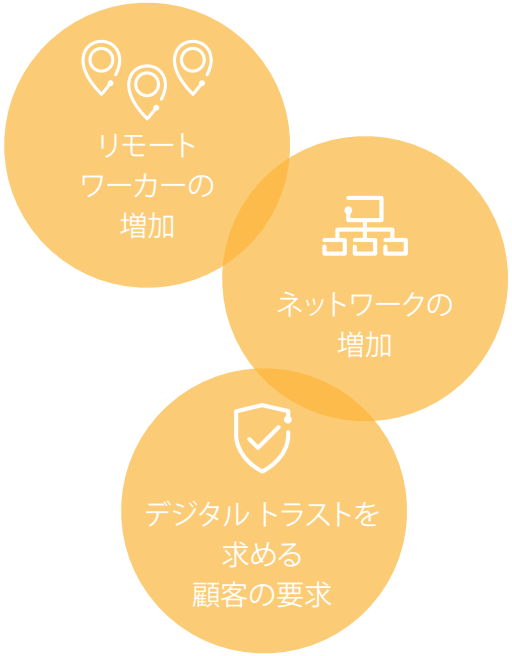


企業は引き続きデジタルトラストに力を入れている

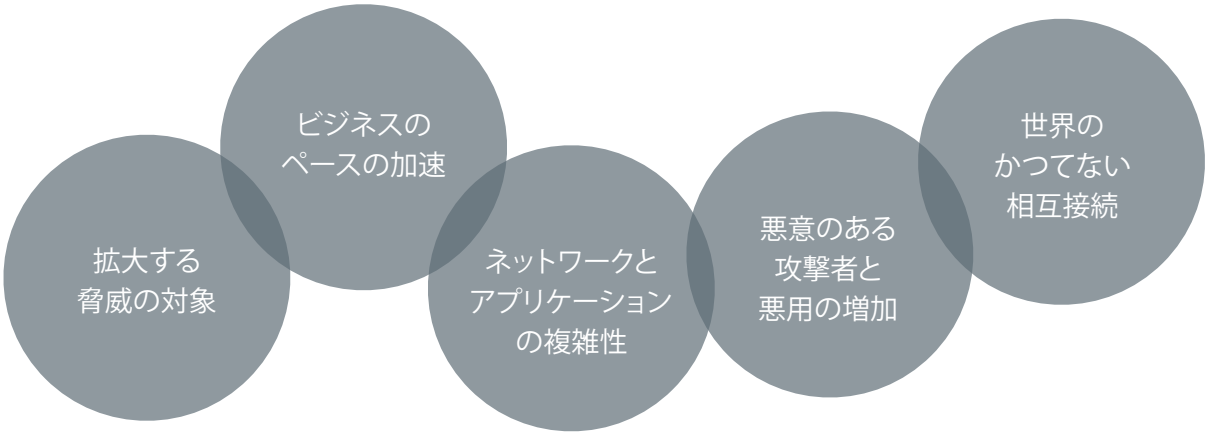
昨年の調査が示していた圧倒的な支持を考えれば、企業が今なおデジタルトラストに力を入れていることは驚くに当たりません。企業の関心を高めている要因のうち、最も重要な原動力は、次の 3 つです。

- リモートワーカーがかつてなく急増している
- ネットワーク数も増加している（エッジネットワーク、パートナーまたは顧客に接続するネットワークを含む）
- 最も重要な項目として、顧客が企業にデジタルトラストを求めている

3 つの主な理由



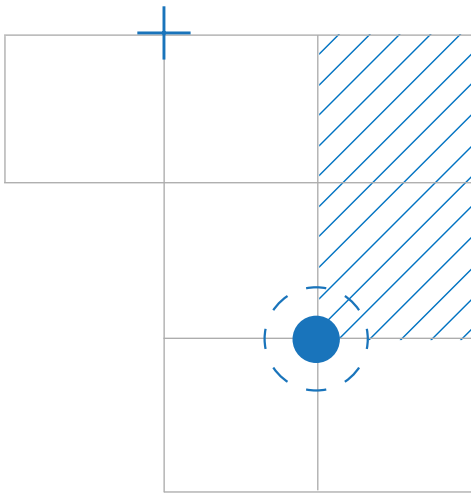
その他の理由



しかしながら、企業はデジタルトラストを確立、監視、管理するのは容易ではないことに気づきはじめています。企業が直面している主な課題は、次の 5 つです。

- **スタッフの専門知識不足。**デジタルトラストはまだ比較的新しい分野です。そのため、すべてのスタッフがデジタルトラストを一元的に導入する方法に精通している訳ではありません。さらに、多くのプライベート PKI は 10 年前に確立されたもので、脆弱でいつ障害が起きてもおかしくないものと思われています。そのことが、チームが本当に必要な専門知識を獲得する妨げとなっています。
- **ネットワークとアプリケーションのさらなる複雑化。**企業のテクノロジーファブリックは複雑化する一方です。ネットワーク側について言えば、企業はもはや従来のデータセンター、リモートオフィス、クラウドという土台の範疇に収まりきらなくなっています。現在のネットワークには、エッジネットワーク、数千人のリモートワーカー、複数のクラウドが含まれます。

  さらに、アプリケーションは単体のアプリケーションから、分散性の高い（多くのサービスが企業の直接管理下に置かれない）マイクロサービスアーキテクチャに移行しました。このような複雑な環境でデジタルトラストを達成するのは至難の業です。
- **企業が保護する必要のある範囲の広大さ。**デジタルトランスフォーメーションの取り組みが進むにつれ、ミッションクリティカルなデジタル資産は増加の一途を辿っています。それに伴って企業が保護する必要がある範囲は急激に拡大します。
- **経営陣からのサポートの欠如。**パンデミックやインフレの影響で経済状況の厳しさが増す中で、経営陣は難しい意思決定を迫られてきました。たとえば、テクノロジー業界の雇用削減数は 2023 年だけで 240,000 人を超えると言われています[1]。このような厳しい環境の中で経営陣のデジタルトラストに対する決意が揺らいだとしても不思議ではありません。
- そして最後に、**暗号化資産の急速な拡大を管理するのは困難で、時間がかかります。**パブリックトラストであろうとプライベートトラストであろうと、電子証明書がトラストを確立する取り組みの土台であることに変わりはありません。しかしながら、企業が現在対応しているような大きな規模で電子証明書を管理するのは困難です。



[1] TechCrunch

デジタルトラスト確立の進捗状況

企業のデジタルトラスト導入状況はどうでしょうか。この問いに完全に答えようとすると、深く複雑な説明が必要になり、一言で言い切ることはできません。しかし、簡単に言えば、企業の導入状況は「良好だが、素晴らしくはない」となります。

その成功の度合いはデジタルフォーカスの各分野によって異なります。そこで、企業の状況を詳しく知るために 4 つの各デジタルトラスト分野を調査しました。

- エンタープライズ
- IoT とコネクテッドデバイス
- ソフトウェア
- 電子署名

エンタープライズトラストの実践

一般的に、企業のデジタルトラストは IT 部門によって管理されます。企業のデジタルトラストで一般的に管理されるデジタルトラストの種類は次の通りです。

- 証明書管理
- ID およびアクセス管理
- メールセキュリティ
- エンドポイントセキュリティ

最も成熟度が高いと推定されるエンタープライズデジタルトラストでさえ、デジタルトラストの取り組みはまだごく初期の段階にあります。自社の取り組みは「きわめて成熟している」と答えたエンタープライズトラスト責任者はほとんどいませんでした（100 社中 2 社のみ）。さらに、87% は取り組みがサイロ化されていると述べました。

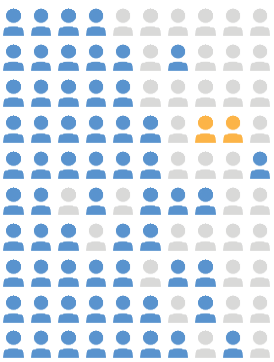
電子証明書は、企業ユーザーと彼らが使用するマシン（ウェブサーバ、スマートフォンなど）の通信を認証し保護する仕組みを提供します。企業のネットワークとユースケースの大規模化と複雑化により、必要な証明書の数は増え続けています。

証明書の管理については、調査した企業の約半数（52%）で IT 部門で管理、3 分の 1（37%）が IT 部門以外で管理、9 社に 1 社（11%）は管理していませんでした。

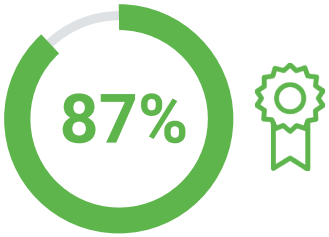
一般的な企業では証明書を発行する部門は 5 部門以下ですが、ほとんどの企業は証明書を発行する部門を増やす必要を感じています。

デジタルトラストの実践がきわめて成熟していると答えた企業は

100 社に 2 社 のみ。



大半の企業は「ある程度」成熟していると回答



エンタープライズトラストの取り組みはサイロ化されていると回答した割合

一般的な企業では証明書発行部門は 5 部門以下

ほとんどの企業は証明書を発行する部門を増やす必要を感じている

証明書の管理部門

IT 部門

IT 部門以外で管理されている

未管理

エンタープライズトラストの実践

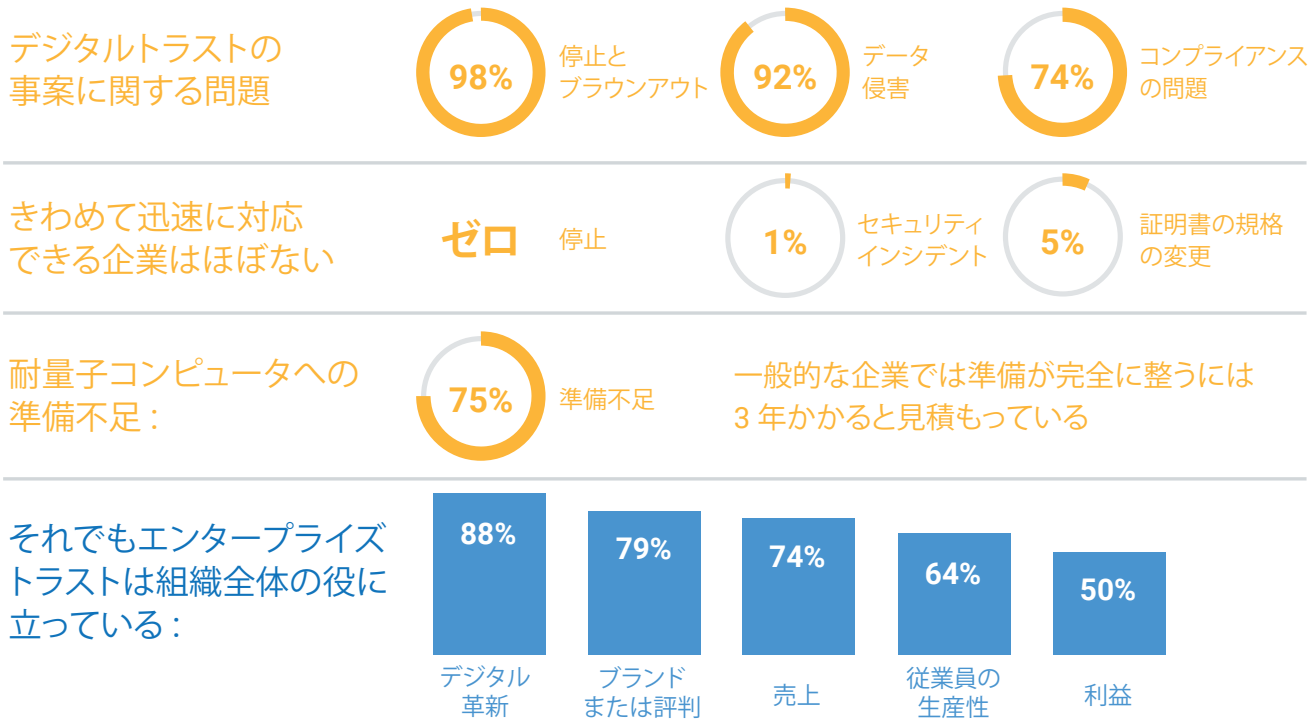
企業のデジタルトラストの取り組み状況はどうでしょうか。結論から言えば、それほどうまくいっていません。回答者はデジタルトラストの事故に関連して次のような問題を報告しています。

- **ほぼすべての回答者（98%）**は少なくとも数回の停止とブラウンアウトを経験している
- **ほとんどの回答者（92%）**がデータ侵害を経験している
- **かなり多くの回答者（74%）**がコンプライアンスの問題を経験している

さらに深く掘り下げ、企業のデジタルトラストの俊敏性を測定しました。

- 停止にきわめて迅速に対応できる企業は**まったくなし**
- セキュリティインシデントにきわめて迅速に対応できる企業は**ほぼなし（1%）**
- 証明書の規格変更にきわめて迅速に対応できる企業は**わずか（5%）**
- **ほとんど（75%）**の企業が量子コンピュータへの備えが不十分で、一般的な企業では準備が完全に整うには 3 年かかると見積もっている

このような問題がある一方で、全体として見れば、エンタープライズデジタルトラスト責任者はその取り組みがデジタル革新からブランド、収益までのさまざまな分野で企業の役に立っていると述べています。



IoT とコネクテッドデバイスのトラストの実践

ここでは、IoT デバイスまたはコネクテッドデバイス（工場用センサー、スポーツウォッチ、住宅用サーモスタットなど）の製造、販売会社に焦点を当てました。組織で次のような業務を担当する責任者に話を伺いました。

- IoT デバイスやコネクテッドデバイスの認証手段に取り組んでいる
- IoT デバイスやコネクテッドデバイスの暗号化を実現している
- IoT デバイスやコネクテッドデバイスのソフトウェアまたはファームウェア更新プログラムに署名している
- IoT デバイスやコネクテッドデバイスを暗号を使用して保護している

IoT とコネクテッドデバイスのデジタルトラストの責任者は、先ほどと同様の「良好だが、素晴らしくはない」と語っています。自社の実践がきわめて成熟していると答えた企業は 7 社に 1 社のみでした。大半の企業は「ある程度」成熟していると答えました。

驚くべきことに、**ほとんどの企業（87%）**は IoT デバイスやコネクテッドデバイスから送られた PII（個人を特定できる情報）を暗号化されていないチャネル上で通信しています。

ほとんどの企業（88%）は CISO（最高情報セキュリティ責任者）を置いています。そのような企業はすべて、電子証明書を使用して現場のデバイスを識別し、強力なユーザー認証を行っています。

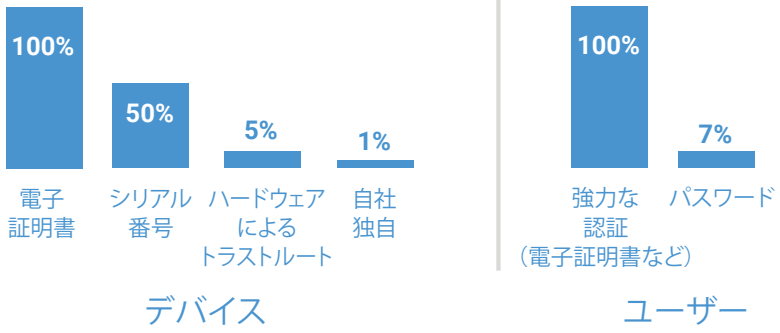
デジタルトラストの実践がきわめて成熟していると答えた企業は
7 社に 1 社 のみ。

大半の企業は「ある程度」成熟していると回答

IoT デバイスやコネクテッドデバイスから得られた PII を暗号化されていないチャネル上で通信している

すべての IoT デバイスやコネクテッドデバイスを管理する、CISO または一元化されたセキュリティ手法が存在する組織の割合

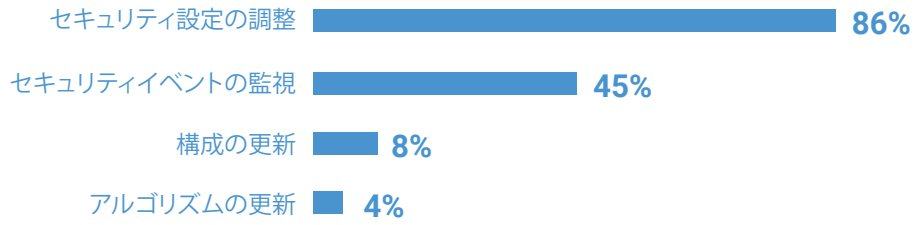
現場でデバイスとユーザーを識別する方法：



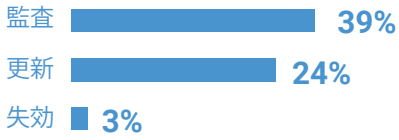
回答者に自社の IoT とコネクテッドデバイスに関する能力をさまざまな分野で評価してもらいました。現場のデバイス管理については回答にばらつきがありました。セキュリティ設定の管理能力は非常に高く、セキュリティイベントの監視も問題ありませんが、デバイスの更新については良くありません。

デバイス ID の管理も全体的にあまり良い結果ではなく、特に証明書の失効化については良くありません。唯一の明るい側面は、ソフトウェア更新プログラムの安全な配信については遅れを取ってはいるものの、ソフトウェアの保護については概ね良好だということです。

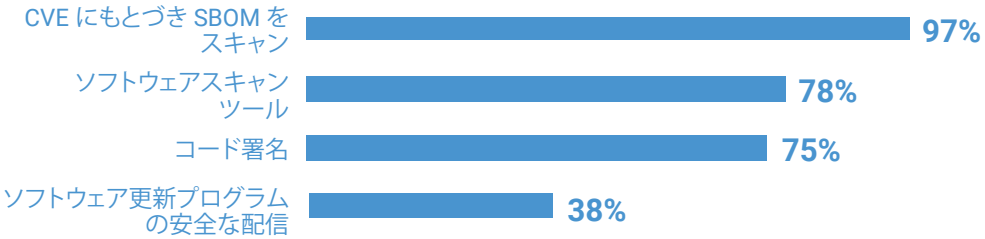
現場のデバイスに対する能力：次の能力がきわめて高い



デバイス ID の管理：



企業がソフトウェアとファームウェア更新プログラムを保護する方法：



IoT とコネクテッドデバイスのトラストの結果

このような能力（とその欠如）について、調査対象の IoT とコネクテッドデバイスのメーカーは少々苦戦していることが分かりました。

- **ほとんどの企業（93%）**がデータ侵害を経験したことがある。その多くはデバイスによってネットワークへの簡単なバックドアが作られてしまったために発生した
- **ほとんどの企業（93%）**は停止とブラウンアウトの両方を経験したことがある
- さらに、最初の点に関連して、**84%** が悪意のある攻撃者による侵入を経験したことがある

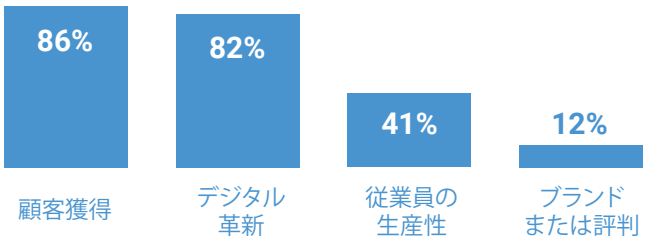
IoT とコネクテッドデバイスのトラストの実践は次のような複数のメリットをもたらしています。

- **86% の企業**が顧客獲得に役立ったと回答している
- **82% の企業**がデジタル革新に役立ったと回答している

とはいえ、IoT とコネクテッドデバイスのメーカーのデジタルトラストの取り組みに改善の余地があることは明らかです。

デジタルトラストの事案に関する問題

それでも IoT とコネクテッドデバイスのトラストは組織全体の役に立っている：



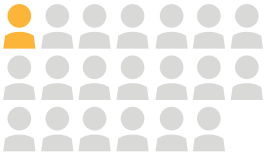
ソフトウェアトラストの実践

ソフトウェアトラストは、ソフトウェア会社が顧客に販売（または配布）するソフトウェアのデジタルトラストを保証します。ここでも調査は「良好だが、素晴らしくはない」という進捗を示しています。ソフトウェアトラストの実践がきわめて成熟していると答えた企業は 20 社に 1 社のみ（5%）でした。企業がコード署名を行う内容にもばらつきがあります。

- **ほぼ全企業（99%）**がソフトウェアソースコードに署名する
- **84%** がソフトウェアバイナリに署名する
- **62%** がビルドスクリプトとインフラ構成に署名する
- **33%** がコンテナおよびサーバレス環境
- **ほとんどの企業（67%）**はコードサイニングの秘密鍵を FIPS-140-2 準拠デバイスに保存しています。

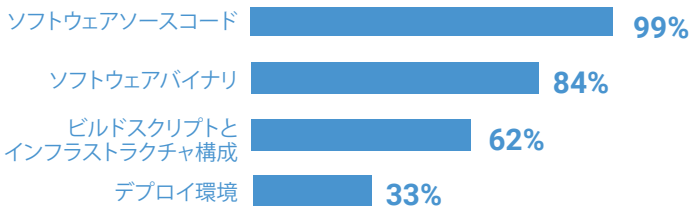
調査対象となった企業のうち、特定のコードサイニングの秘密鍵が危殆化した場合に、その鍵に関連するすべてのアプリケーションをきわめて迅速に発見できると回答した企業はありませんでした。

デジタルトラストの実践がきわめて成熟していると答えた企業は
20 社に 1 社 のみ。

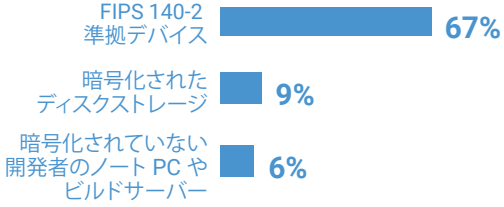


大半の企業は「ある程度」成熟していると回答

コード署名を行う内容：



コードサイニング秘密鍵の保存先：



コードサイニング秘密鍵が危殆化された場合、その鍵を使用して署名していたすべてのアプリケーションをすばやく、簡単に発見できる企業は**なし**

ほぼ全員が開発したソフトウェアのソフトウェア BOM（SBOM）を日常的に作成している。

ほぼ全員がサードパーティソフトウェアのリスク、セキュリティ、法的な要件を設定している。

ソフトウェアトラストの結果

ソフトウェアに関連するコンプライアンス遵守についての企業の状況はどうでしょうか。きわめて良い結果を出しているのは 8 社中 1 社のみです。また、ソフトウェアトラストの事故について多数の問題が報告されています。

- **86%** がデータ侵害を経験した
- **80%** がソフトウェアビルドインフラの侵害を経験した
- **79%** がコードサイニング証明書の期限切れによってソフトウェアが動作しなくなった
- **78%** がマルウェア、その他の脆弱性を含むソフトウェアを出荷した
- **75%** がコード署名やマルウェア検知に関連してリリース期限に間に合わなかった

顧客は企業のソフトウェアの完全性に依存していますが、コード署名に必要なすべての鍵を保護するのは非常に骨の折れる作業です。

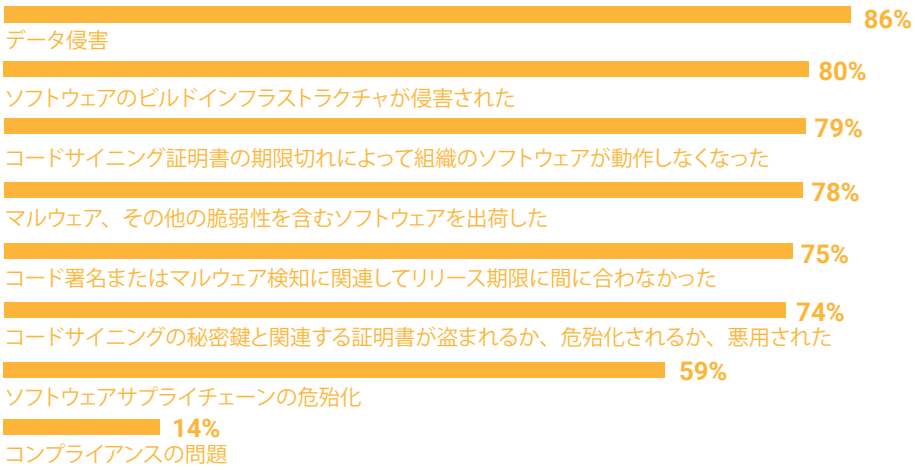
自社が開発したソフトウェアに使用されているソフトウェアコンポーネントのリストを簡単に生成できる企業はほとんど存在しません。

とはいえ、全体的に見れば、ソフトウェアトラスト責任者はその取り組みが 2 つの方法（デジタル革新と従業員の生産性）で企業の役に立っていると述べています。

ソフトウェアについて規制遵守の取り組みできわめてよい結果が得られている割合

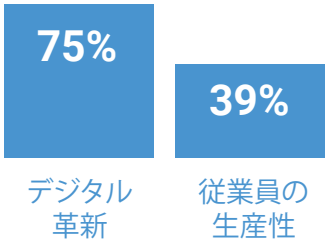
大半がある程度の結果が得られている。

デジタルトラストの事案に関する問題



開発したソフトウェアのすべてのコンポーネントと構成のリストを作成するのはきわめて簡単だと答える割合

それでも IoT とコネクテッドデバイスのトラストは組織全体の役に立っている：



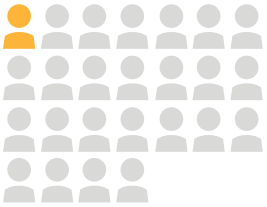
電子署名トラストの実践

ドキュメントサイニング証明書では、個人、チーム、組織が各種ファイル形式の文書に電子的なデジタル署名を加えて、所有権を証明し、文書が改ざんされないことを保証し、機密情報を保護することができます。

自社の電子署名トラストの成熟度を評価してもらったところ、電子署名トラストの実践はきわめて成熟していると回答した企業は 25 社に 1 社（4%）でした。これは 4 分野で最低の評価です。このセグメントの 1 つの特徴は、電子署名は IT 部門ではなくビジネス部門（法務、人事、調達など）の担当者によって管理されるということです。また、基本的な電子署名と証明書ベースの電子署名の違いを理解しているのは 8 社に 1 社のみでした。

- **約半数（48%）**が文書（法務、営業、調達など）に e シールを使用している
- **ほとんど（86%）**が信頼されたサードパーティによって発行された証明書によるデジタル署名を使用して署名者を検証している

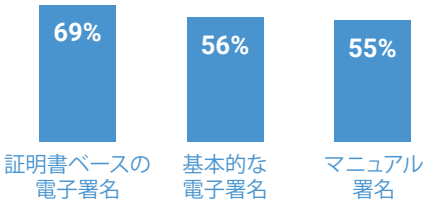
デジタルトラストの実践がきわめて成熟していると答えた企業は
25 社に 1 社 のみ。



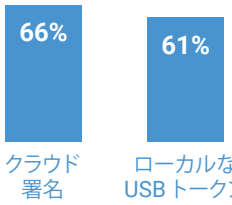
大半の企業は「ある程度」成熟していると回答

基本的な電子署名と証明書ベースの電子署名の違いについてよく理解している

使用される署名の種類：



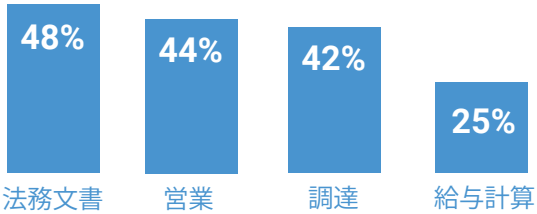
電子署名を使用する人によって使用された署名の種類



信頼されたサードパーティによって発行された証明書による電子署名を使用して署名者を検証している割合

約半数が文書に e シールを使用している

一般的な使用例：



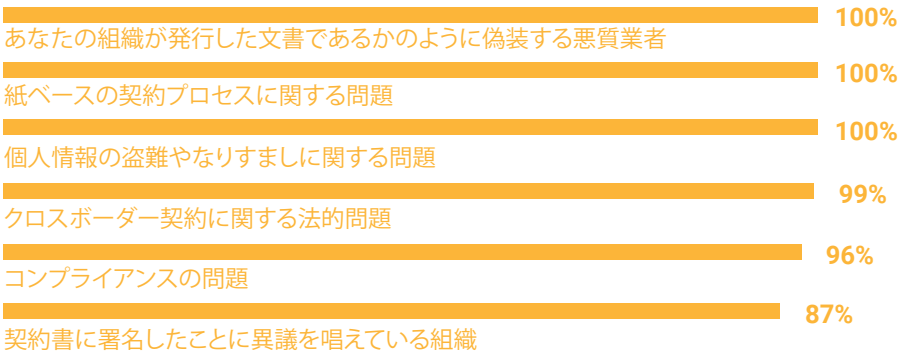
電子署名トラストの結果

このグループでは、トラストの事故に関連する問題のインシデント数が最多でした。

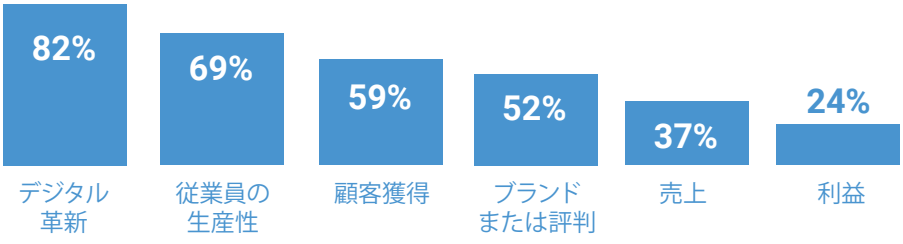
- **100%** がその組織が発行した文書であるかのように偽装する悪質業者を報告している
- **100%** が紙ベースの契約プロセスに関する問題を報告している
- **100%** が個人情報の盗難やなりすましに関する問題を報告している
- ほぼすべて（**99%**）がクロスボーダー契約に関する法的問題を報告している
- **96%** がコンプライアンスの問題を報告している
- **87%** の組織が契約書に署名したことに異議を唱えている

このような問題がある一方で、全体的には、その取り組みが企業のデジタル革新、生産性、顧客獲得その他に役立っていると述べています。

デジタルトラストの事案に関する問題



それでもエンタープライズトラストは組織全体の役に立っている：



デジタルトラストの専門家の言葉

ここまで、すべての企業を合わせた結果について見てきました。ところが、同じグループ内でも平均より良い結果を出す企業と平均よりも悪い結果を出す企業があることに気づきました。

この違いが気になったため、結果を階層化して比較することにしました。そのために、結果を測定可能なすべての質問（「侵害を見たことがありますか」「インシデントにどれだけ迅速に対応できますか」などの質問）を採点しました。良い結果にはプラス点、悪い結果にはマイナス点を付け、点数を集計して各回答者の合計点を計算しました。

全カテゴリの点数が上位 33% に入った企業には、「デジタルトラストリーダー」の称号を与えました。 下位 33% の企業は「デジタルトラストラガード（遅滞者）」です。

私たちは、4 つのデジタルトラスト分野のそれぞれにおける、この 2 つの群の結果と実践の違いを理解するためにさらに深く調査しました。

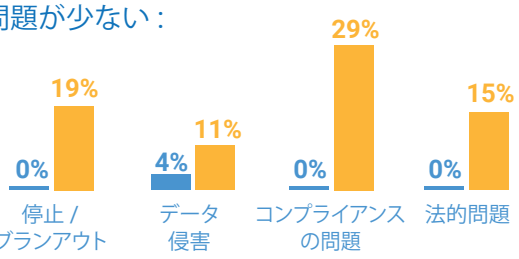
エンタープライズトラスト

まず、エンタープライズトラストについて見ていくと、リーダーの結果の方が大幅に優れていることが分かります。エンタープライズトラストに関連する問題の数は非常に少ないです（停止なし、データ侵害ほぼなし、コンプライアンスまたは法的問題なし）。

リーダーの約 4 分の 3（74%）が停止にきわめて迅速に対応できると回答していますが、同じ回答をしたラガードはわずか 59% です。

リーダーは耐量子コンピュータの備えができていると回答している割合がラガードの 6 倍です（**ラガードの 11% に対してリーダーは 59%**）。

エンタープライズトラストに関連する問題が少ない：



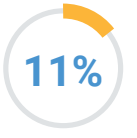
停止にすばやく対応

きわめて迅速に対応すると答えたリーダーの割合

きわめて迅速に対応すると答えたラガードの割合

PQC の準備が進んでいる

準備できていると答えたリーダー

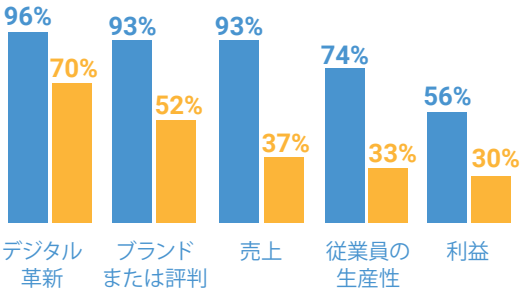


準備できていると答えたラガード

PQC への準備が整うのが早い

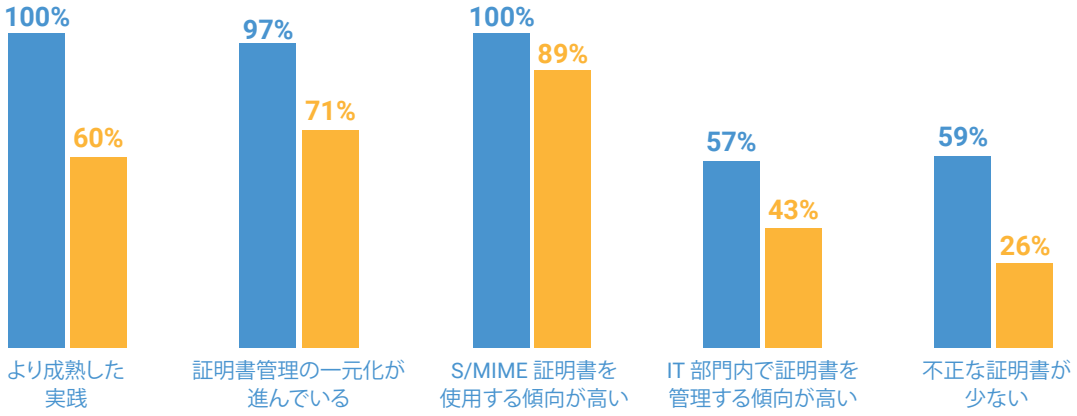
リーダーは準備に 2 年、ラガードは 3 年かかる

エンタープライズトラストは次の方法で組織に大いに役立った：



リーダーは何が違うのか

まず、エンタープライズトラストリーダーの 100% がきわめて成熟したエンタープライズトラストの実践を行っていると述べています。一元化も進んでおり、メール通信の保護に S/MIME 証明書を使用し、証明書の管理は IT 部門内で行っています。また、矛盾するようですが、不正な証明書の数も少ないと報告しています。

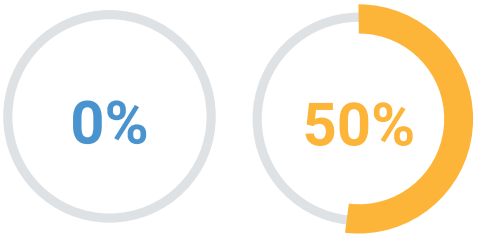


IoT とコネクテッドデバイスのトラスト

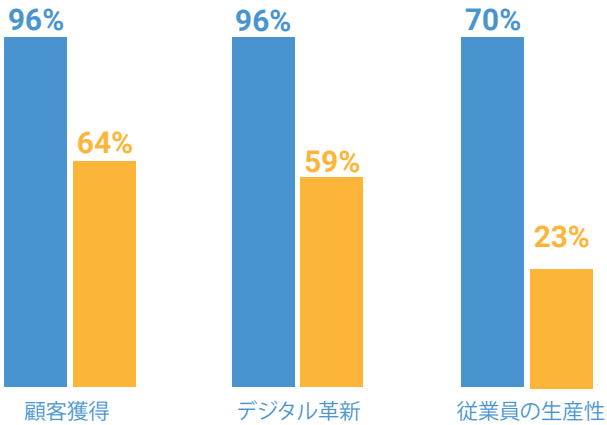
次に、IoT とコネクテッドデバイスの専門家について調査しました。ここでも、リーダーの結果の方がラガードの結果をはるかに上回っています。IoT とコネクテッドデバイスによるコンプライアンスの問題を経験したリーダーは皆無であるのに対し、ラガードの約半数（**50%**）がそれを経験しています。

IoT とコネクテッドデバイスのトラストが組織の役に立っていると回答した割合もリーダーの方が多く、ほぼすべての回答者（96%）が顧客獲得、デジタル革新の役に立ったと述べ、ほとんどの回答者（70%）が従業員の生産性に役立ったと述べています。ラガードではそれぞれ、64%、59%、23% に過ぎません。

コンプライアンスに関する問題が少ない



IoT トラストは次の方法で組織に大いに役立った：

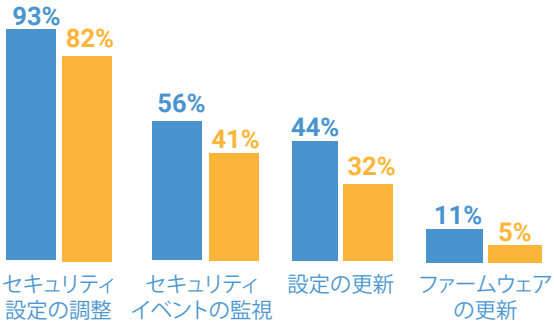


実践の違いは何か

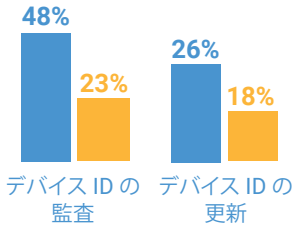
まず、リーダーは現場のデバイスに対して変更したり監視したりする能力に優れています。また、デバイス ID の監査や更新に関する能力も優れています。

最後に、IoT トラストの問題に対して十分に準備できていると答えたラガードは皆無でしたが、リーダーの 19% がそのように回答しました。

現場のデバイスを変更する能力が高い：



次の分野の能力が高い：



IoT トラストの問題に対して準備が整っている

ソフトウェアトラスト

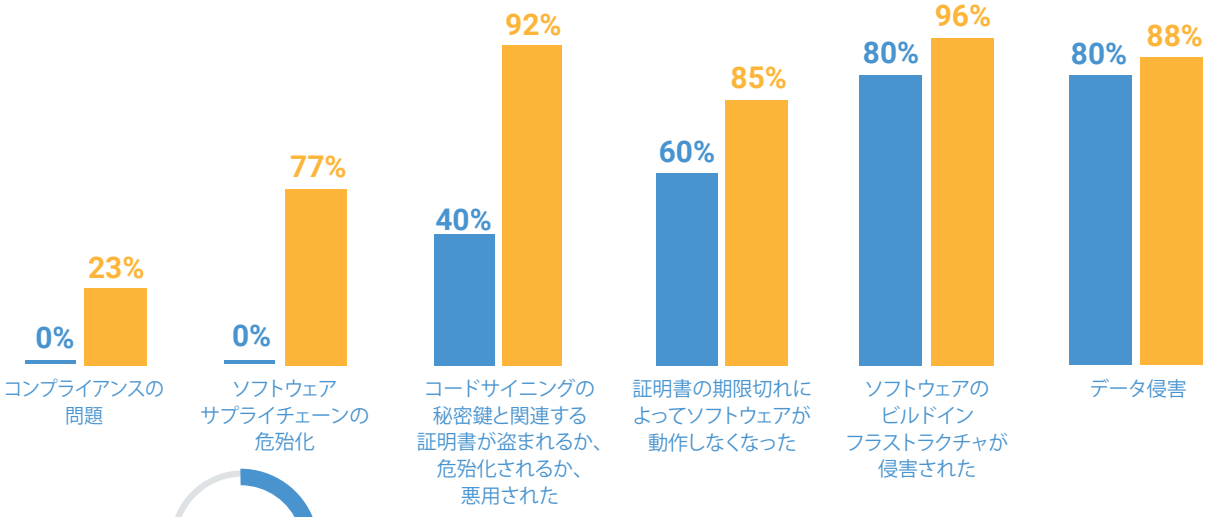
次に、ソフトウェアトラストの専門家について見ていきます。ここでも、リーダーの結果はラガードの結果より優れており、ソフトウェアトラストの事故による問題件数が大幅に少なくなっています。たとえば、コンプライアンスの問題やソフトウェアサプライチェーンの危殆化を経験したリーダーは皆無だったのに対し、ラガードはそれぞれ 23%、77% の企業が経験しました。

さらに、5 社中 1 社の企業**(20%)**は、きわめて成熟したトラストの実践をしていると述べています（ラガードは 0%）。

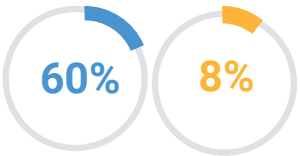
また、リーダーはコンプライアンス遵守についても優れています（ラガードの 8% に対して 60%）。

リーダーはラガードと比べ、そのソフトウェアトラストの取り組みが組織全体に良い影響を与えておりデジタル革新、顧客獲得、従業員の生産性などの分野で役に立っていると回答する割合が多くなっています。

ソフトウェアトラストの事故についてリーダーが経験する問題は少ない

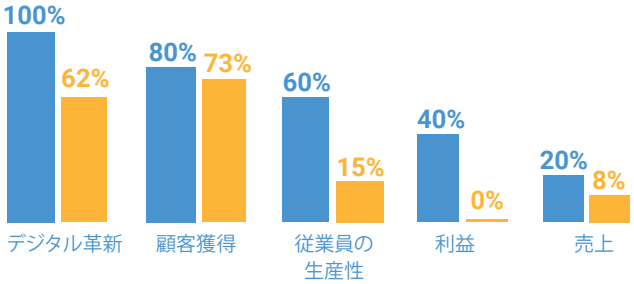


きわめて成熟したソフトウェアトラストの実践をしているリーダーの割合（ラガードは 0）



リーダーは規制遵守についてきわめて良い結果を出している

ソフトウェアトラストは次の方法で組織に大いに役立った：



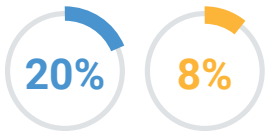
リーダーを際立たせているものは何か

リーダーは、暗号鍵にアクセスするために正式な承認プロセスを使用する割合がラガードの 2 倍です（ラガードの 38% に対して、リーダーは 80%）。

また、開発したソフトウェアのすべてのコンポーネントとその構成のリストを作成するのはきわめて簡単だと回答する割合が非常に多くなっています（ラガードの 8% に対して、リーダーは 20%）。

暗号鍵にアクセスするために
正式な承認プロセスを
使用する傾向が強い

リーダーにとって、開発したソフトウェアの
すべてのコンポーネントと構成のリストを
作成するのはきわめて簡単



電子署名トラスト

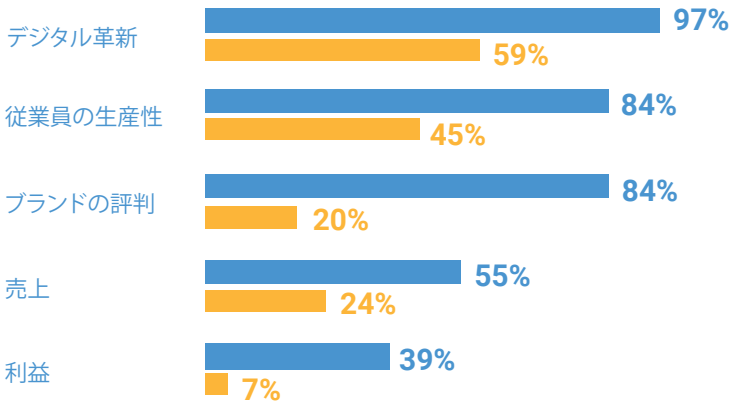
最後のグループでは、電子署名のトラストの専門家について見ていきます。電子署名のトラストは技術畑ではないスタッフ（人事部門、法務部門、営業部門などの責任者）によって管理されることが多くあります。IT 部門が関与しない場合、電子署名のトラストの取り組みの詳細を管理するのに役立つ技術的な深さが不足するため、それが結果に表れています。

たとえば、きわめて成熟した電子署名トラストの実践を採用していると回答したリーダーはラガードよりも多いですが、実際の数（10%）はまだ少数です。また、リーダーは経験する電子署名トラストの問題も少なく、ラガードよりも組織に役立っていると回答する割合が多くなっています。

きわめて成熟した
電子署名トラストの
実践をしている
リーダーの割合
（ラガードは 0）

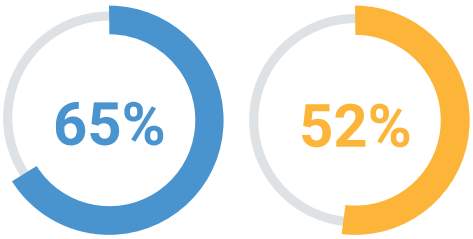
リーダーは電子署名トラストの問題の数が少ない：

電子署名トラストは次の方法で組織に大いに役立った：



リーダーの特徴とは

これらの違いはある 1 つの重要な性質に集約されます。電子署名と e シールの方針とガバナンスに関する理解、導入、管理について、リーダーの方が成熟度が高いのです。



電子署名と e シールの方針とガバナンスに関する理解、導入、管理について、リーダーの方が成熟度が高い

デジサートの見解

脅威の現状が拡大するとともに、デジタルトラストの最前線に立つ企業と遅れを取っている企業との格差も拡大しています。リーダーとラガードは自らの立ち位置を自覚していますが、本当のリスクは誤った安心感を抱いている可能性のある中間層にあります。独りよがりの安心感によってこのギャップが拡大すれば、深刻な結果を招く可能性があります。

全体、およびエンタープライズ IT、ソフトウェア、デバイス、文書のトラストなどの各分野におけるデジタルトラストの取り組みを最適化するために組織は何をすべきでしょうか。

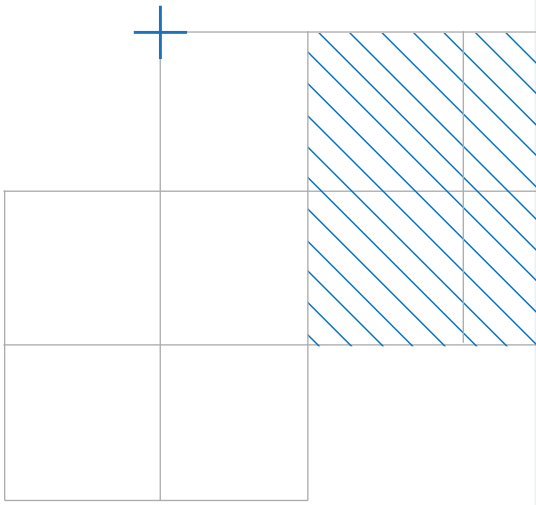
デジサートは、デジタルトラストをお届けする世界有数のプロバイダーです。個人と企業が、それぞれのデジタルフットプリントの安全性を信頼してオンラインで取引できるよう取り組んでいます。20 年以上にわたってデジタルトラストに携わってきた経験から、リーダーが実証した成功を模範したい企業へのアドバイスは次の通りです。

インベントリを作成する

「見えないものは管理できない」という金言はデジタルトラストの管理にも当てはまります。企業内でデジタル ID と暗号鍵がどのように作成され、保護され、使用されているかについて全体像を把握します。それには、手作業でビジネスプロセスを発見する方法と、テクノロジーを使用して環境を継続的にスキャンし、IT 資産管理システムなどのその他のソースからデータを取り込む方法があります。

ポリシーを制定する

デジタルトラストの対応を支援するためにポリシー上で考慮すべき点は数多くあります。組織はリモートワーカーと従来のオフィスワーカーのデバイスおよびユーザー認証を安全に行うためのポリシーを制定する必要があります。特に、医療機器メーカーなどの規制の厳しい業界では、コンプライアンス遵守に必要なポリシーをすべて特定しましょう。ビジネスクリティカルなソフトウェアを発行している組織の場合、ソフトウェアサプライチェーンのセキュリティを保護するためのポリシーを策定します。特に、機密データや規制データを処理するクラウドネイティブなワークロードについては、ゼロトラストイニシアチブを確立するか、進化させます。以上の例は、組織内の暗号通信や PKI（公開鍵基盤）の使用を管理するための基本的なポリシーに加えて制定するものです。



PKI 管理を一元化する

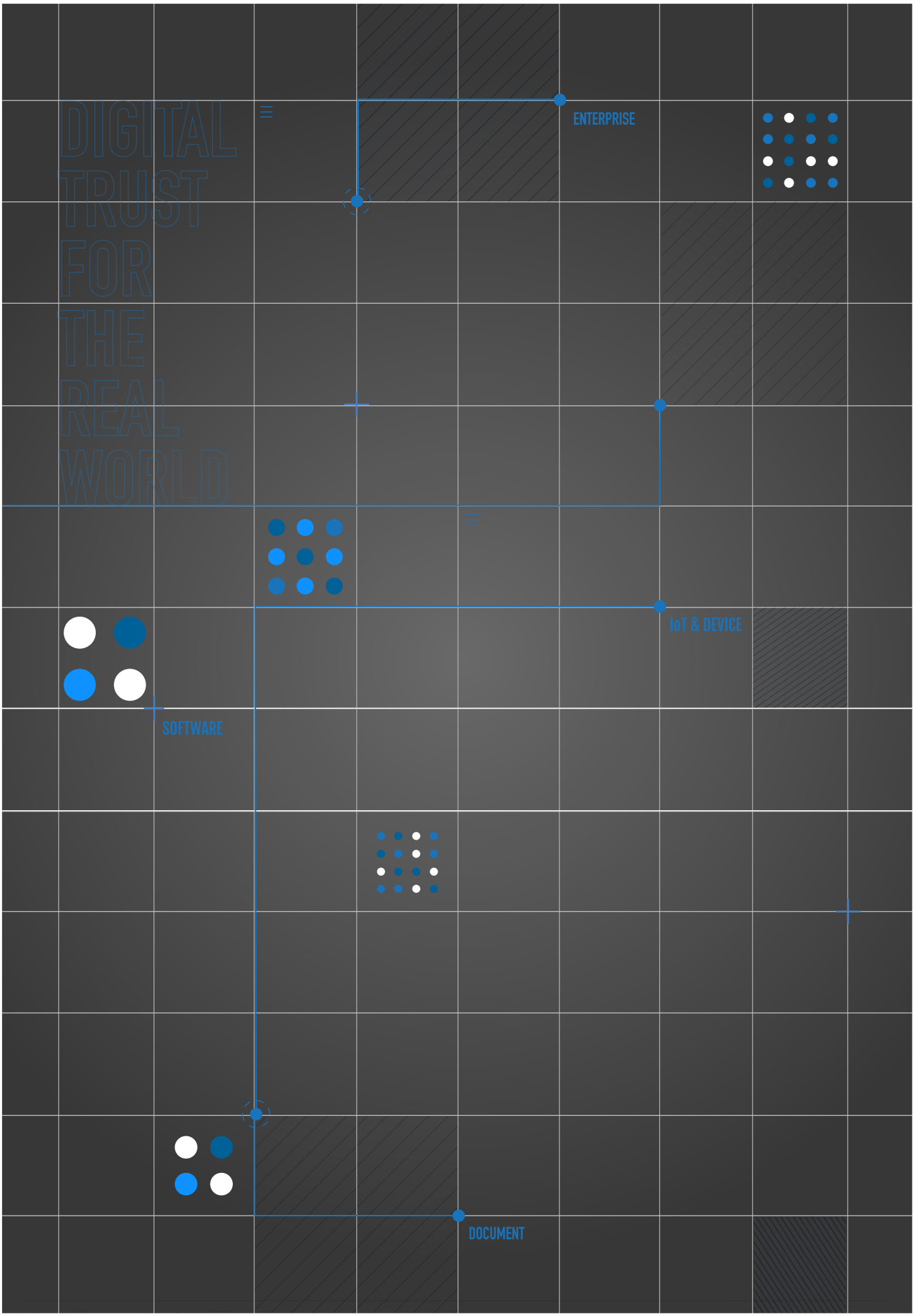
組織にはある程度の「暗号アジリティ」、すなわち、暗号資産を迅速に更新、修正する能力が必要です。将来の混乱を防ぎ、リスクを最小限に抑えるため、電子証明書と PKI を一元管理して自動化するツールを導入します。 このアプローチには、セキュリティの向上、効率化、管理の簡素化など、複数の利点があります。

ビジネスへの影響に基づいて優先順位を付ける

インベントリを見直し、ビジネスクリティカルなアプリケーションやプロセスに関連している資産を特定します。これらが最初にレベルアップしたい領域です。デジタルトラストをサポートするタスクを合理化するソリューションを導入する作業に移る前に、セキュリティ脆弱性に対処します。たとえば、IT チームの手を借りることなく、ユーザーがセキュアなリモートアクセスのために自動的かつ簡単にデバイスを登録できるようにするなどです。サーバー証明書を素早く安全に発行およびインストールすることでデータと通信を保護し、クラウドのセキュリティを向上します。

まとめ

デジタルトラストに重点を置いている組織は、ブランドの強化、サイバーセキュリティリスクの低減、運用効率の向上を実現しています。そのような組織は強固なセキュリティ対策と透明性の高いガバナンスにより、顧客、パートナー、利害関係者からの信頼を得ています。デジタルトラストを確立することで、複雑な規制にうまく対応し、コンプライアンスを確実に達成し、法的リスクや財務リスクを低減できます。したがって、データを保護し、レジリエンスを高め、現代のデジタル環境における新たな脅威に対応できるのです。


DIGITAL
TRUST
FOR
THE
REAL
WORLD
ENTERPRISE
IoT & DEVICE
SOFTWARE
DOCUMENT