STATE OF DIGITAL TRUST

PILLARS OF TRUST

C- LEVEL, DIRECTOR
MANAGER INSIGHTS

DIGITAL TRUST READINESS
SCORE

1245.56°
753234.72°

IDENTITY

AUTOMATION

433.6°
24567.76°

ID 7021.4

THREATS

SECURITY ALERT

ZERO TRUST

ENTERPRISES
EMPLOYEES
CUSTOMERS

6578.854°
6785.77°

GLOBAL STUDY

NOVEMBER 2022

digicert®

2022 年
デジタルトラストの実態調査

私たちは、人と人が直接会う世界から常時デジタルでつながった世界に急速に移行しています。デジタルトランスフォーメーションがこの移行を加速しています。パンデミックによっても、加速されました。しかし、この新しい世界でどのように信頼（トラスト）を構築すればよいのでしょうか。以下について、どのように行いますか。

- つながっている人々（とデバイス）が正当だと確認する
- 消費しているデータが安全か見分ける
- 自分たちがセキュリティ侵害や DDoS 攻撃にさらされていないことを保証する
- 実行しているアプリケーションとサービスが危殆化していないことを確認する

簡単なことではありません。この新しい世界は脅威の対象となる領域を大幅に拡大し、セキュリティの低下によるコストが爆発的に増大しました。とりわけ、法的コスト、規制コスト、修復コスト以外を考えると、最大のコストは顧客ロイヤルティと企業のブランドの喪失でしょう。Forbes Insights レポートによると、全組織の半数近く（46%）が、サードパーティによるセキュリティ侵害によって評判とブランドが傷つく経験をしています [1]。

これは、デジタルトラストの問題を表面化させました。IDC のリサーチディレクター、Jennifer Glenn 氏によると、デジタルトラストはつながった世界を保護するための基盤で、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です。

本質的に、デジタルトラストはデジタル世界に全面的に参加する自由をもたらします。

デジタルトラストを提供する世界有数のプロバイダーであるデジサートは、個人や企業がデジタル世界における操作に対し安全性を信頼して、オンラインで取引ができるよう取り組んでいます。デジサートは、グローバル組織のデジタルトラストの認識具合と、組織のデジタルトラストへの取り組みの進捗をよりよく理解する役割を担っています。

デジサートの 「2022 年 デジタルトラストの実態調査」では、全世界の企業、従業員、消費者がデジタルトラストに関してそれぞれどのように受け入れているのか調査しています。

[1] The Reputational Impact of IT Risk – Forbes Insights

デジタルトラストとは何か

IDC のリサーチディレクター、Jennifer Glenn 氏によると、デジタルトラストはネットでつながる世界を保護するための基盤で、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です。

デジタルトラストは、以下の四大要素を基盤として成り立っています。

1. 特定の技術や産業における信頼を定める標準・規定
2. （実在性の証明、データの完全性、暗号化により）信頼を担保する電子証明書の生成もしくは検証によるコンプライアンスとオペレーションが、標準化・規制団体にり定められた要件を満たしていることを保証
3. トラスト管理は、企業が正常に証明書ライフサイクルを管理しており、その使用について一元的に可視化および管理していることを保証
4. 接続される信頼は、ソフトウェア、デバイス、コンテンツの利用により起こる、より複雑なサプライチェーンにまで拡張される

デジタルトラストは、これら 4 つの主要な構成要素で構成されています。企業は、これらのアクティビティの一部または全部の管理について、第三者に委ねることや内部で行うことができます。

「デジタルトラストはネットでつながる世界を保護するための基盤である。」

—Jennifer Glenn、IDC リサーチディレクター。

デジタルトラストの重要性

デジタルトラストの必要性は、回答者の共感を呼びました。全企業（100%）がデジタルトラストは重要だと言い、大多数（90%）がきわめて重要だと述べています。実際にそれほど重要なため、3 分の 2 近くの企業がそれまでのベンダーへの信頼を無くした後、ベンダーの乗り換えを経験しています。そしてほぼすべて（99%）の企業が、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思っています。そのうち半数近く（47%）は、そうなると信じています。

企業の従業員も全面的にデジタルトラストに賛同しています。100% の従業員が重要だと述べ、86% はきわめて重要だと述べています。企業内の自分の役割として、99% の企業においてベンダーへの信頼を無くした場合、ベンダー乗り換えを検討し、約半数（51%）が「多分」乗り換えると述べています。

最後に、3 分の 2（68%）の消費者がデジタルトラストは重要だと述べ、3 分の 1（36%）がデジタルトラストはきわめて重要だと述べています。実際、半数（47%）の消費者が、過去に信頼を失った企業との取引を停止したことがあります。今後、84% の消費者が乗り換えを検討し、57% が乗り換えがありうるとしています。顕著なのは、消費者が裕福なほどデジタルトラストは重要だと述べていることです。平均を上回る収入のある 58% の消費者が、デジタルトラストは重要だと述べています。

調査方法

2022 年 9 月、ダラスに本社を置く Eleven Research が「2022 State of Digital Trust」調査を実施しました。調査は、世界中の 400 の大手企業と 400 の消費者を対象に電話とメールにより行われました。

大手企業

1,000 人以上の従業員を抱える 400 の企業の IT、情報セキュリティ、DevOps の上級管理職と経営幹部を対象に調査を行いました。回答は以下のように広範囲なものでした。図 A（5 ページ参照）

消費者

幅広い年代、性別、政治的志向、経済状態にある世界の 400 の消費者（同地域）を対象に調査しました。図 B（5 ページ参照）

100
北米
100
EMEA
50
中東
50
中南米
100
アジア太平洋

図 A

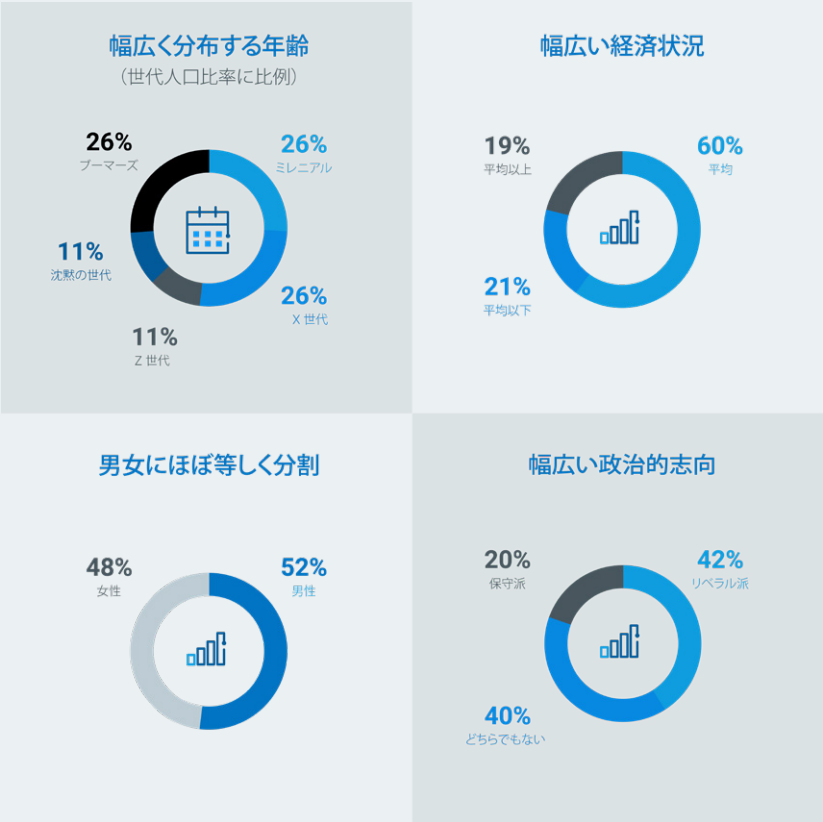
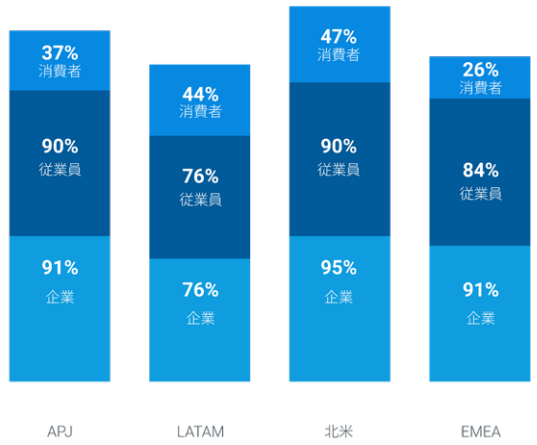

幅広く分布する年齢
（世代人口比率に比例）
26%
ブーマーズ
26%
ミレニアル
11%
沈黙の世代
26%
X 世代
11%
Z 世代
幅広い経済状況
19%
平均以上
60%
平均
21%
平均以下
男女にほぼ等しく分割
48%
女性
52%
男性
幅広い政治的志向
20%
保守派
42%
リベラル派
40%
どちらでもない

図 B

多岐に渡るデジタルトラストの重要性

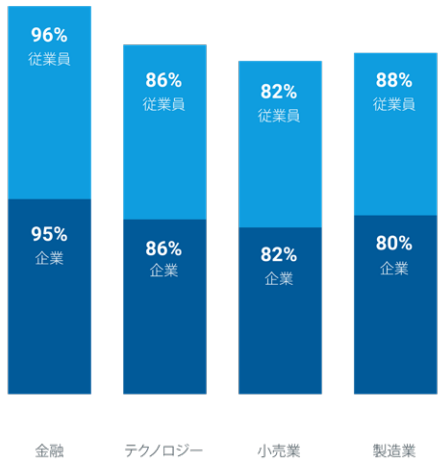
企業、従業員、消費者はデジタルトラストが重要なことには賛同していますが、重要度は属性の種類によります。

地域別のデジタルトラストの重要性の特徴



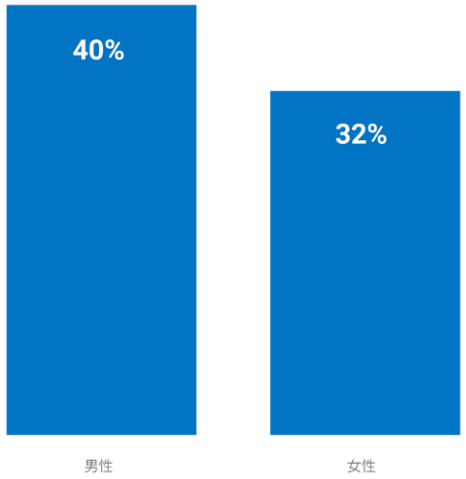
中南米では、企業と従業員がデジタルトラストはきわめて重要という感覚の点で後れを取っています。APJ（日本を含むアジア太平洋）と EMEA（ヨーロッパ、中東およびアフリカ）では、消費者が後れを取っています。EMEA では厳格な EU GDPR（一般データ保護規則）法が 2018 年に制定されており、消費者の 26% が、デジタルトラストはきわめて重要というのは驚きだったと述べています。

業界別のデジタルトラストの重要性の特徴



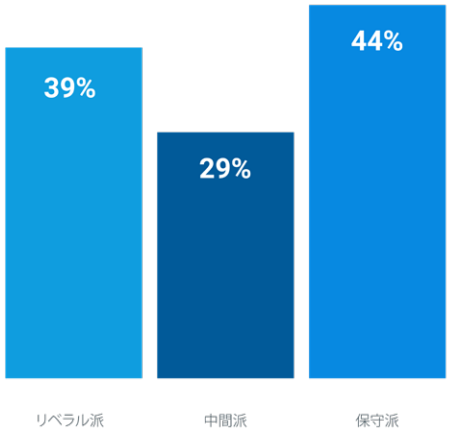
予想どおり、金融がデジタルトラストはきわめて重要と述べる傾向が高いです。

男女別のデジタルトラストの重要性の特徴（消費者）



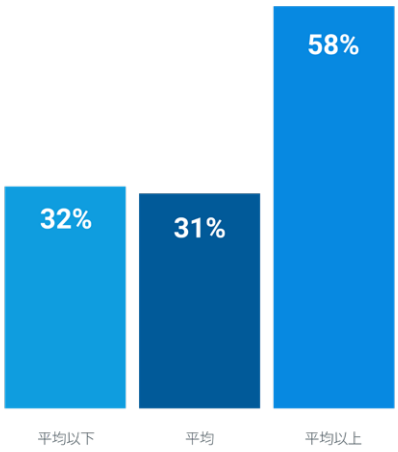
男性消費者の方が女性消費者よりもデジタルトラストをより重要としています。

政治的志向別のデジタルトラストの重要性の特徴（消費者）



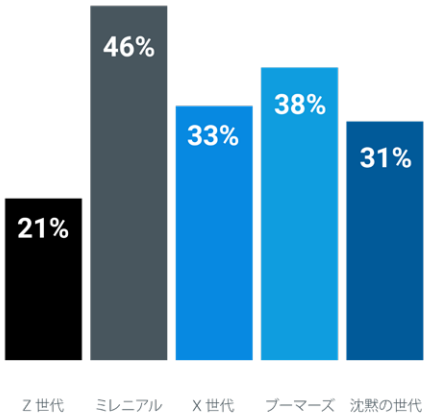
最後に、これにはリベラル派と保守派が同意できるということです。両者は、デジタルトラストはきわめて重要と述べる傾向があります。

収入別のデジタルトラストの重要性の特徴（消費者）



また、平均以上の収入のある消費者にとって、デジタルトラストはさらに重要となっています。

世代別のデジタルトラストの重要性の特徴（消費者）



興味深いことに、最も若い 2 つの世代（唯一のデジタル世代）では、一方がデジタルトラストはきわめて重要と述べる傾向が最も低く、もう一方が最も高くなっています。

デジタルトラストへの関心を高める原動力とは

デジタルトラストへの関心は普遍的ですが、この関心を高めているのは何でしょうか。私たちは、さまざまな要因を見つけました。

データの重要性の高まり。回答者によると、これが最大の要因です。なぜでしょうか。複利率 23% でデータが増大しているためです [2]。言い方を変えます。世界で 2021 年末時点の 97 ゼタバイトのデータが蓄積されるまでに 70 年かかりました。ほんの 4 年後の 2025 年までに、世界のデータはほぼ倍増の 174 ZB になります。2025 年までに、地球上の一人一人が 20,000 ギガバイトを超えるデータをもつことになります。

しかしながら、これはデータ量だけのことではなく、このデータがいかに重要かということです。データは個人を特定できる情報の宝庫です。情報には、私たちが買ったもの、訪問した場所、健康記録、ソーシャルメディア、写真などがあります。

拡大する脅威の対象。企業は、データセンター、オフィス、リモートサイトからなる比較的静的な自社ネットワークをはるかに複雑なハイブリッドネットワークに転換してきました。これらの新しいネットワークは、データセンター、オフィス、リモートサイトを接続しつつ、何千もの在宅勤務サイト、複数クラウド、デジタルデバイス、エッジネットワーク、IoT デバイスを追加しています。

この新しいエッジレスネットワークには、桁外れに多くの攻撃ポイントがあります。

顧客からの期待。前セクションで見たように、全企業（100%）と 68% の消費者がデジタルトラストを重要なものと評価しています。企業も消費者も、ある企業への信頼を無くした場合、競合他社に乗り換える傾向があります。デジタルトラストは、実在する資産になりました。

悪意のある攻撃者の増加。毎年、悪意のある攻撃者の数は増えています。これには以下のものが含まれます。

- ブラックハットハッカー
- サイバー犯罪者
- サイバーテロリスト
- ハクティビスト
- 内部攻撃者
- 国家的な攻撃者
- スリルを求める人、荒らし

悪意ある攻撃者の増加の証拠は、2021 年に IC3 が受けた苦情の数が最多になったことから分かります。2020 年から 7% 増加して 847,376 件もの苦情が報告されました [3]。

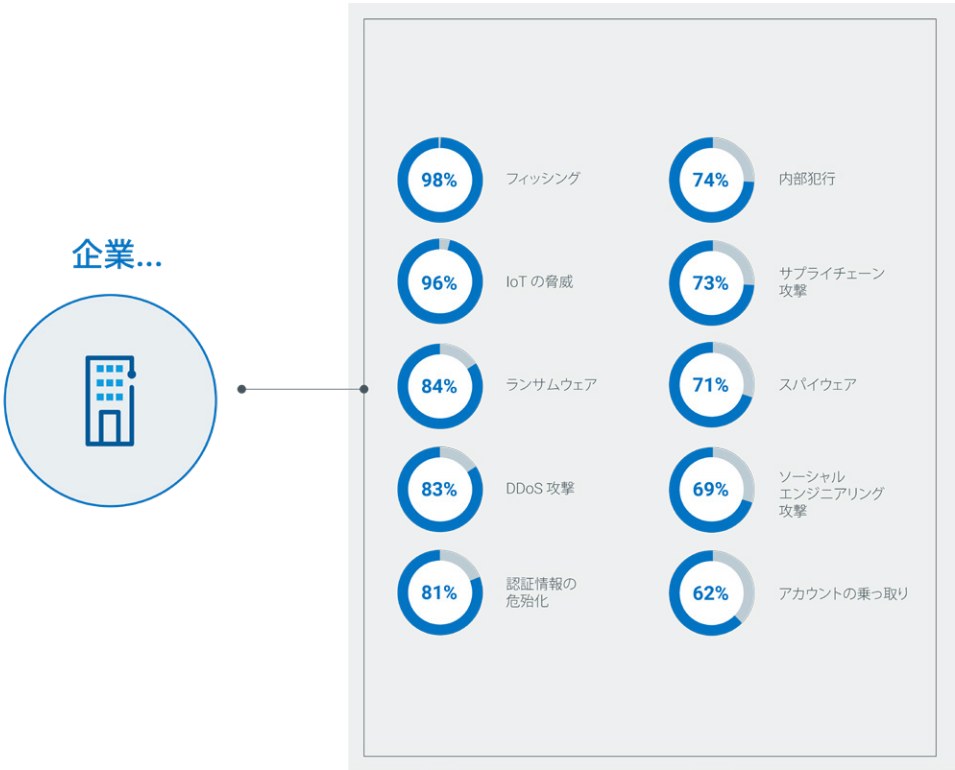
[2] Big Growth Forecasted for Big Data - IDC

[3] FBI Internet Crime Complaint Center (IC3)

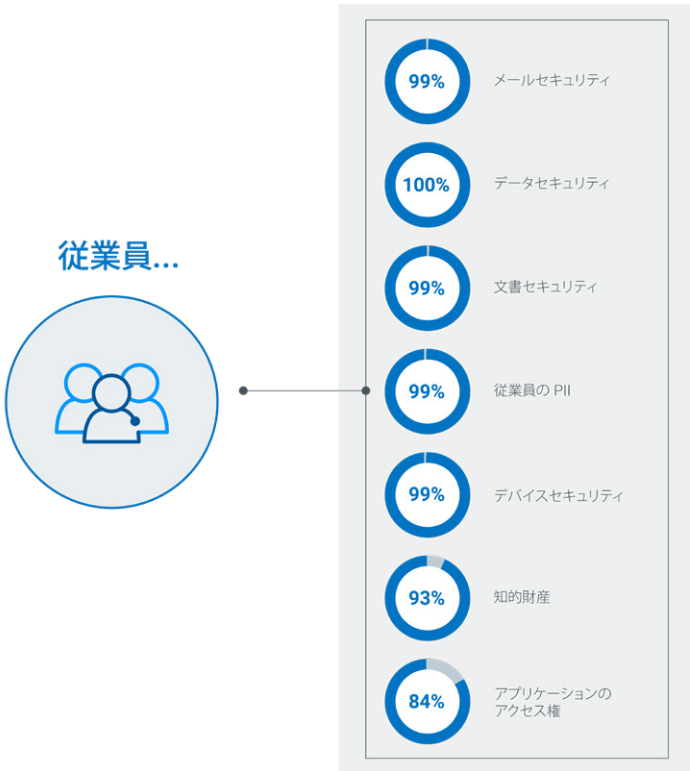
何が危うくなっているか

企業は何を保護していますか。回答者の全企業（100%）は、顧客ロイヤルティを重要なものとして挙げています。顧客がある企業への信頼を無くした場合に競合他社に乗り換える可能性を考えれば、これは納得のいくことです。

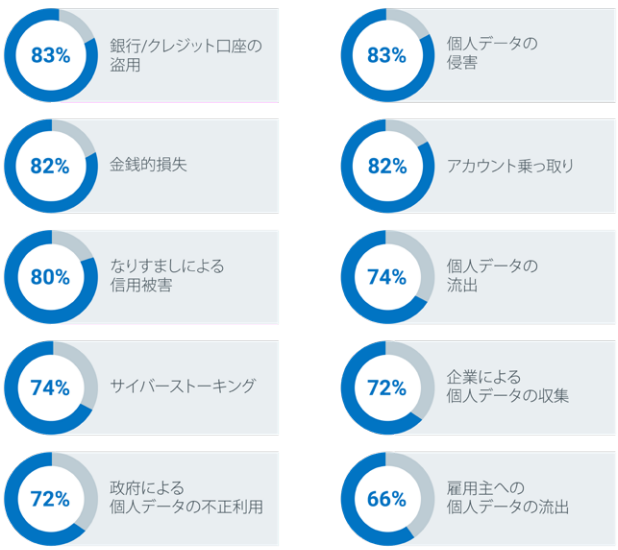
回答者が明かした最も恐れている攻撃のタイプを順番に示します。

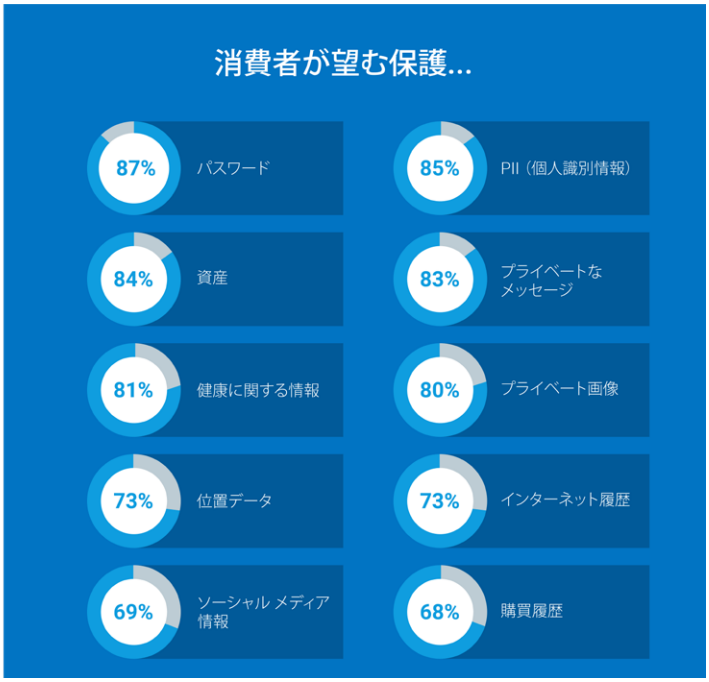


企業の従業員には別の懸念があります。自分の個人情報です。



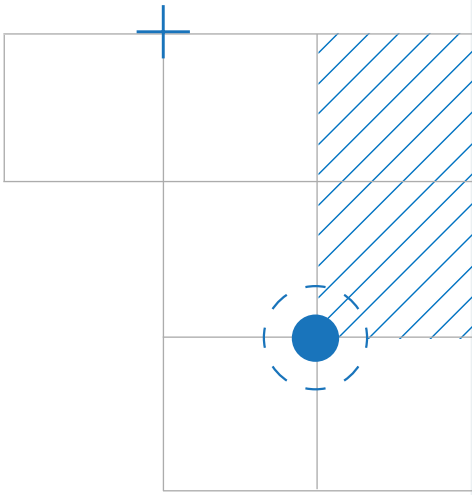
最後に、消費者にはさまざまな懸念があります。





消費者にとって最も重要なこと（パスワード、個人を特定できる情報（PII）など）の保護に役立てるという点で、企業が消費者と同じ考えだったかどうか調べてみました。 実際には、消費者データを危殆化するすべての攻撃はメール攻撃から始まります[4]。ただ、企業がさまざまな消費者を守る試みをしているものの、フィッシング攻撃からの保護は対策手段という点で下から 2 番目と見なされていました。ただ実際のところ、企業はフィッシングを最も懸念する攻撃と見なしてはいました。

そのため、企業は消費者にとって最も重要なことに力を入れてはいるものの、消費者が望むセキュリティレベルを達成する道のりは長いとも言えます。

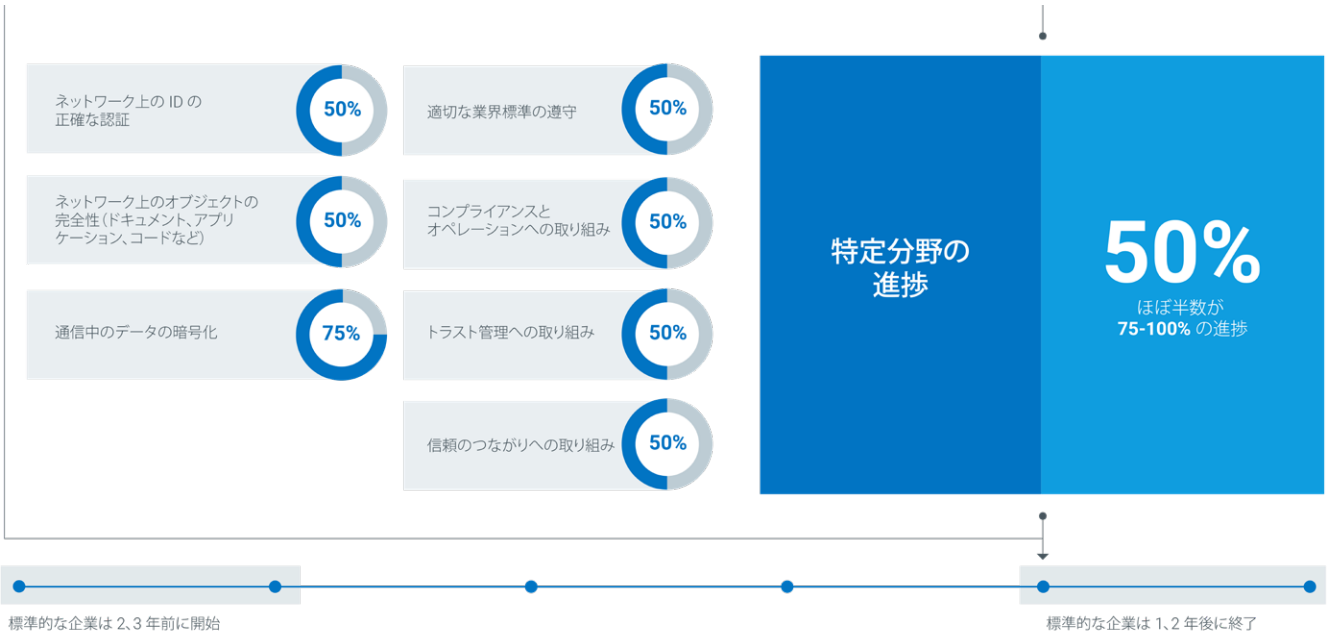


[4]Why Your Business Needs Better Email Security - Guardian Digital

企業はデジタルトラストをどのように最適化しているか

企業はデジタルトラストに取り組んでいます。標準的な組織は、2、3 年前からデジタルトラストに取り組み始め、これまでに 75%（またはそれ以上）の進捗まで来ています。これらの標準的な組織はデジタルトラストへの対応を 1、2 年後には完了するでしょう。

デジタルトラストにはさまざまな側面があります。企業がどこまで進んだかを見るために、さらに掘り下げて調べてみました。



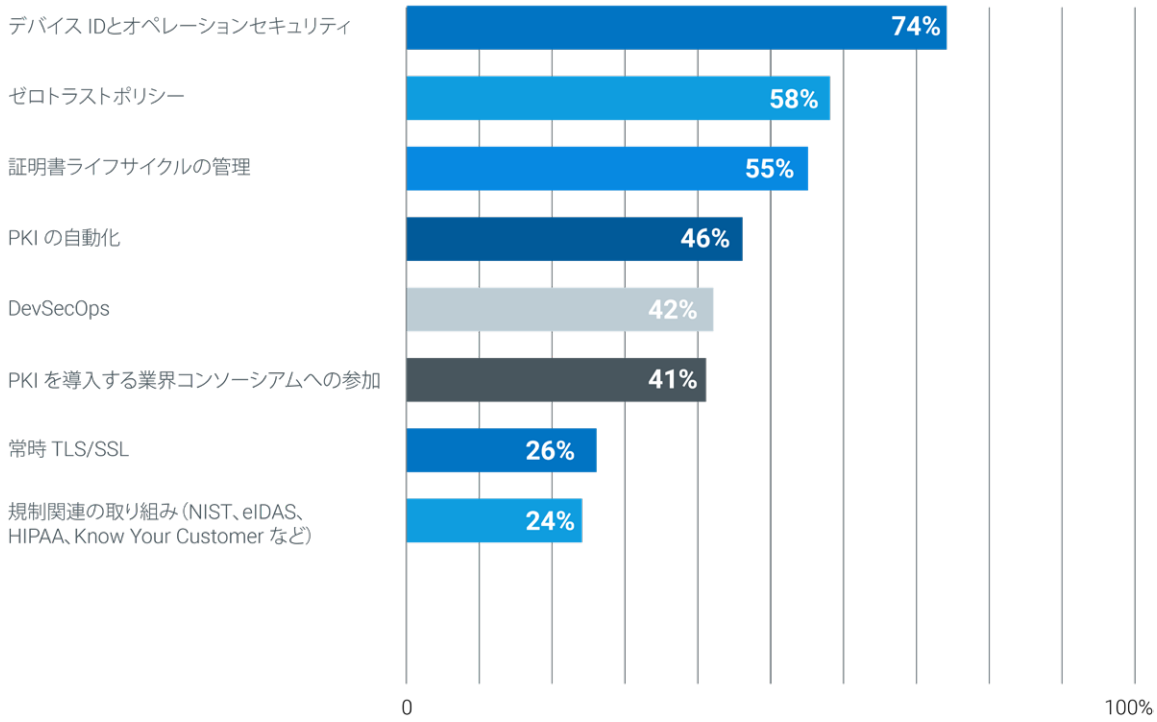
デジタルトラストの目標：企業は、デジタルトラストの第一の目標は顧客ロイヤルティだと明確に述べています。全企業がこの目標を重要と見なし、企業の第一の目標としました。しかし、他の目標もあったのです。

デジタルトラストの課題：企業はデジタルトラストへの対応を進めていますが、容易ではありませんでした。IT 面で挙げられる第一の課題は電子証明書の管理で、それには全企業が重要と見なしていました。規制の遵守と膨大な保護対象範囲の処理が 99% で僅差の 2 位です。課題として上げるのは複雑性で、複雑でダイナミックなマルチベンダーネットワークを保護する必要があることです。しかし、スタッフの専門知識は不足しています。

デジタルトラストの実践：幅広い取り組みが、企業のデジタルトラストに影響する可能性があります。ほとんどの企業がこれらの取り組みに少なくとも多少は関わっており、企業が完全に導入済みの取り組みを確認することが役に立っています。

1 位はデバイス ID とオペレーションセキュリティで、現在 74% の企業が完全に導入しています。ゼロトラストポリシーがその次で、58% の企業が完全導入しています。その次に、大半の企業（55%）で導入されている取り組みは、証明書ライフサイクル管理です。その他は以下の通りです。

Q22: デジタルトラストにおける次の各手法について、どの程度対応を進めていますか？
（すでに導入済み）

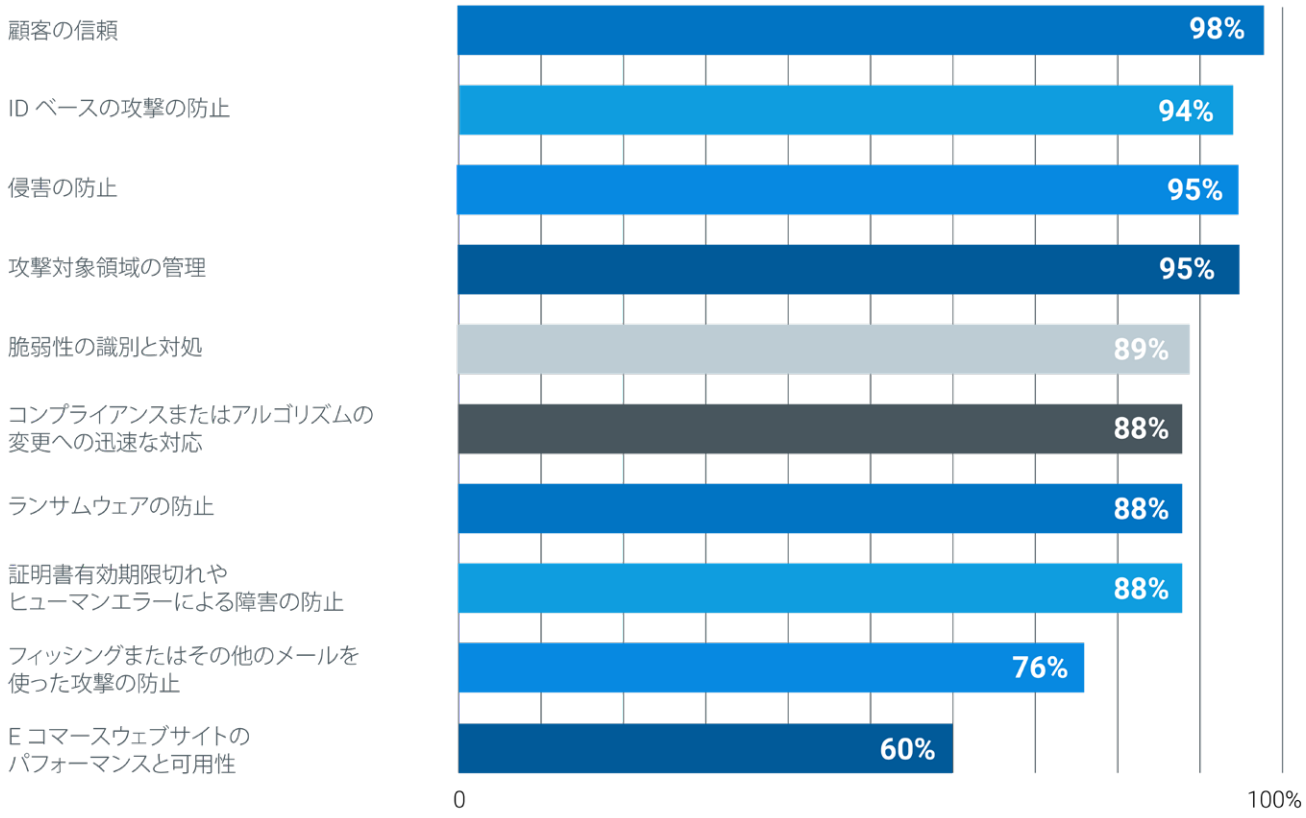


企業はデジタルトラストの指標をどうしているか

企業は、デジタルトラストに関する様々な目標指標に対して全体的に非常に良い成果を出しています。第一の目標（顧客からの信頼）を例にします。98% の企業がこの目標について好結果を出し、61% がきわめて良い結果を出しています。95% が侵害の防止についても好結果を出し、51% がきわめて良い結果を出しています。94% が ID ベースの攻撃について好結果を出し、50% がきわめて良い結果を出しています。

実際、私たちが調査した 10 の指標のうちの 8 つについて、少なくとも 8 社中の 7 社が好結果を出していると述べました。フィッシングまたはその他のメールを使った攻撃の防止と E コマースウェブサイトのパフォーマンスと可用性だけが後れを取っていて、それぞれ 76% と 60% です。

Q23: デジタルトラストにおける次の各指標について、どの程度の結果が得られていますか？
（ある程度/非常によい結果が得られている）



改善を期待する顧客

全企業（100%）が、デジタルトラストは顧客にとって重要だと報告しており、91% の企業は顧客がデジタルトラストはきわめて重要と見なしていると述べています。

そのため、顧客が自身のデジタルトラストをどう認識しているかを把握することは不可欠です。企業の観点からは、顧客が従来の企業のデジタルトラストより現在のものを信頼していると 99% の企業が述べている点は良いことです。ほぼ 4 分の 3（73%）の企業が、著しく良いと述べています。

それでは、企業の側からはどう感じているのでしょう。同様の楽観論を共有しているでしょうか。実際、その数はほぼ同じです。企業がやり取りしている会社への信頼度を評価するよう依頼されると、98% が従来よりも現在の方が高いと述べ、76% がきわめて高いと述べています。

ですが、これは B2B のやり取りの場合です。B2C ではどうでしょう。その数字は B2B ほど楽観的ではありません。取引している組織のデジタルトラストの評価は従来よりも高いと回答するのは半数以下で、54% が改善の余地があると述べています。

「91% の顧客は、
デジタルトラストは
きわめて重要と
考えている。」

北米の結果

北米（米国とカナダ）は、デジタルトラストをきわめて重要と評価している点で世界をリードしています。これは、企業、従業員、消費者のいずれにも当てはまります。

顕著なのは、北米の消費者が、アジア太平洋を除く世界のどの地域の消費者よりもサイバー脅威（銀行口座やクレジットカード情報にアクセスされ、金銭を盗まれるような）を最も懸念していることです。（APAC の消費者の 91% がこれらの脅威を懸念しています。北米では 85%、EMEA では 77%、LATAM では 78% です。）

こうしたことは、北米の企業に対して消費者が評価した高スコアに表れています。デジタルトラストの成功という点で、31% の北米の消費者が、取引している企業をより著しく信頼していると述べています。APAC ではその中間の 19% の消費者がそうです。これは南米の消費者の 24% に匹敵し、APAC と EMEA ではそれぞれわずか 19% と 15% です。

APAC の結果

全般的に、アジア太平洋ではデジタルトラストをきわめて重要と見なしています。北米を除く他のどの地域よりも、アジア太平洋の人々はデジタルトラストにより力を入れています。

ひとつには、APAC の消費者が、世界のどの地域の消費者よりもサイバー脅威（銀行口座やクレジットカード情報にアクセスされ、金銭を盗まれること）をより懸念しているためです。（APAC の消費者の 91% がこれらの脅威を懸念しています。北米では 85%、EMEA では 77%、LATAM では 78% です。）

デジタルトラストの成功という点で、その中間の 19% の APAC の消費者が、取引している企業をより著しく信頼していると述べています。北米と南米ではそれぞれ 31% と 24% の消費者がそう回答しますが、EMEA の消費者はわずか 15% しかそう感じていません。

中南米（LATAM）の結果

全般的に中南米は、デジタルトラストの重要性を考慮する点で、世界から後れを取っています。

ひとつには、中南米の消費者が、一般の消費者よりもサイバー脅威（銀行口座やクレジットカード情報にアクセスされ、金銭を盗まれるような）を懸念していないためです。（わずか 78% の LATAM の消費者しかこれらの脅威を懸念していません。APAC では 91%、北米では 85%、EMEA では 77% です。）

デジタルトラストという点で、LATAM の消費者が比較的高い成功をしていると述べ、24% の LATAM の消費者が、取引している企業をより著しく信頼していると述べています。比較すると、北米の消費者の 31%、APAC の 19%、EMEA の 15% がそう述べています。

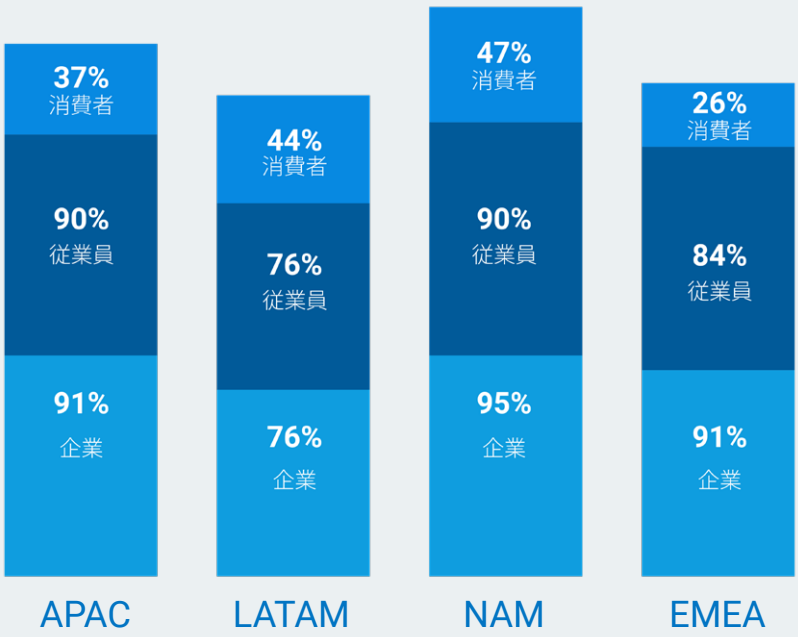
EMEA の結果

最も厳格なプライバシー法（GDPR）のいくつかを定める地域である、EMEA の消費者は驚くほどデジタルトラストに関心がありません。全般的には、EMEA はデジタルトラストの重要性の評価の仕方という点で、3 位にランクされています。しかし、データを掘り下げてみると、EMEA は企業レベルでは強い関心をもち、従業員レベルでは中程度の関心をもっています。デジタルトラストの重要度が北米のほぼ半分なのは、消費者レベルだけです。

これは、サイバー脅威への懸念と相関関係があります。EMEA の消費者のサイバー脅威（銀行口座やクレジットカード情報にアクセスされ、金銭を盗まれるような）への懸念は最低レベルです。わずか 77% の EMEA の消費者しかこれらの脅威を懸念していません。対して、LATAM では 78%、北米では 85%、APAC では 91% です。

これも、取引している企業への信頼が近年増加した（わずか 15%）と述べている EMEA の消費者の割合が比較的低いことと相関関係があります。このことは、APAC（19%）、LATAM（24%）、北米（31%）から後れを取っています。

地域別のデジタルトラストの重要性の特徴



デジタルトラストの専門家の言葉

前のセクションで見たように、企業はデジタルトラストへの取り組みで非常に良い結果を出しているようです。これが普遍的な事実かどうか、平均よりも著しく良い結果か悪い結果を出す企業のグループがあるのかどうか、私たちは確かめたいと思いました。

これを調査するため、指標の質問への回答を採点しました。

採点ガイド

- まったくいい結果が得られていない　-2
- あまりいい結果が得られていない　-1
- どちらとも言えない　0
- ある程度の結果が得られている　+1
- 非常によい結果が得られている　+2

次に、各回答者の総スコアを計算するために各個人の 3 つのスコアを加えました。回答者を 3 つの層に分けました。

企業のデジタルトラスト層

- 最上位層（全回答者を 3 分割した上位部分のスコア）
- 中間層（3 分割した中央部分）
- 最下位層（3 分割した下位部分）

この階層化によって、優良企業（最上位層）と劣位企業（最下位層） の間の劇的な違いがいくつか明らかになりました。

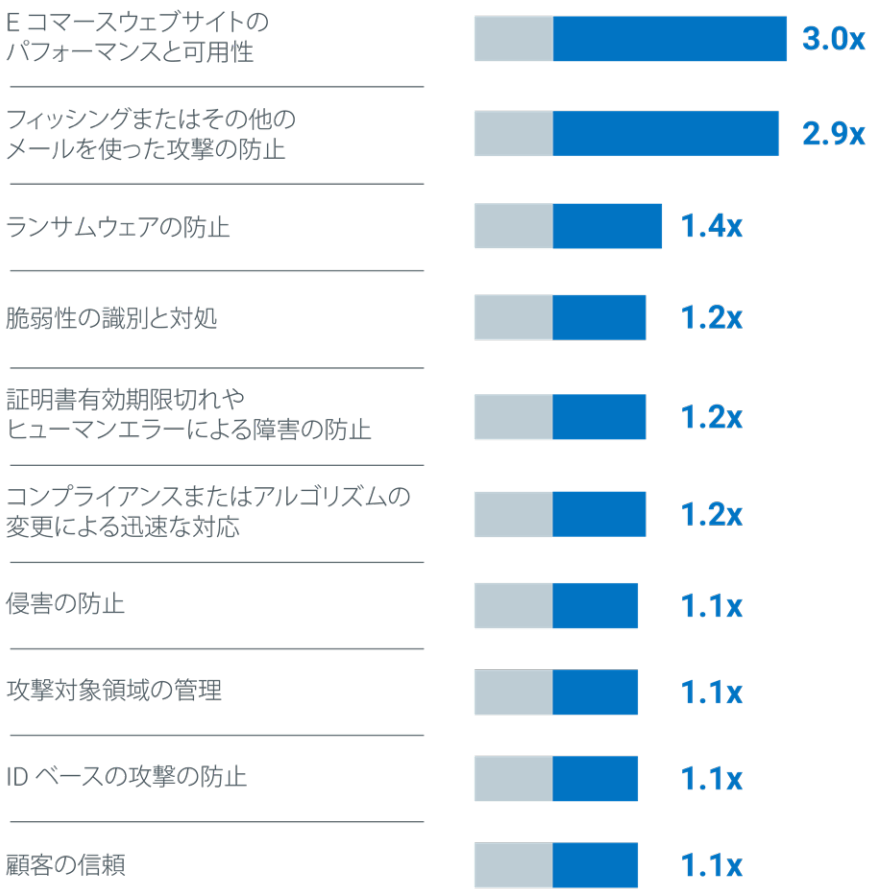
どのくらい良いか

最上位層がデジタルトラスト指標について、よりよい結果を出していることは自明です。そもそも、そのように回答者を層に分けたのです。興味深いことは、最上位層が最下位層よりもどのくらい良い結果を出しているかだけです。たとえば、E コマースウェブサイトのパフォーマンスと可用性については 3 倍もの最上位層の企業が良い結果を出していると述べ、フィッシングまたはその他のメールを使った攻撃の防止については 2.9 倍もの企業が良い結果を出していると述べています。最上位層の企業は、各指標について最下位層より 10% から 300% 良い結果の範囲に入ります。

最上位層組織の顧客は
最下位層組織の顧客に比べて、
組織をより著しく信頼する傾向が
高いです。

[2]Big Growth Forecasted for Big Data - IDC
[3]FBI Internet Crime Complaint Center (IC3)

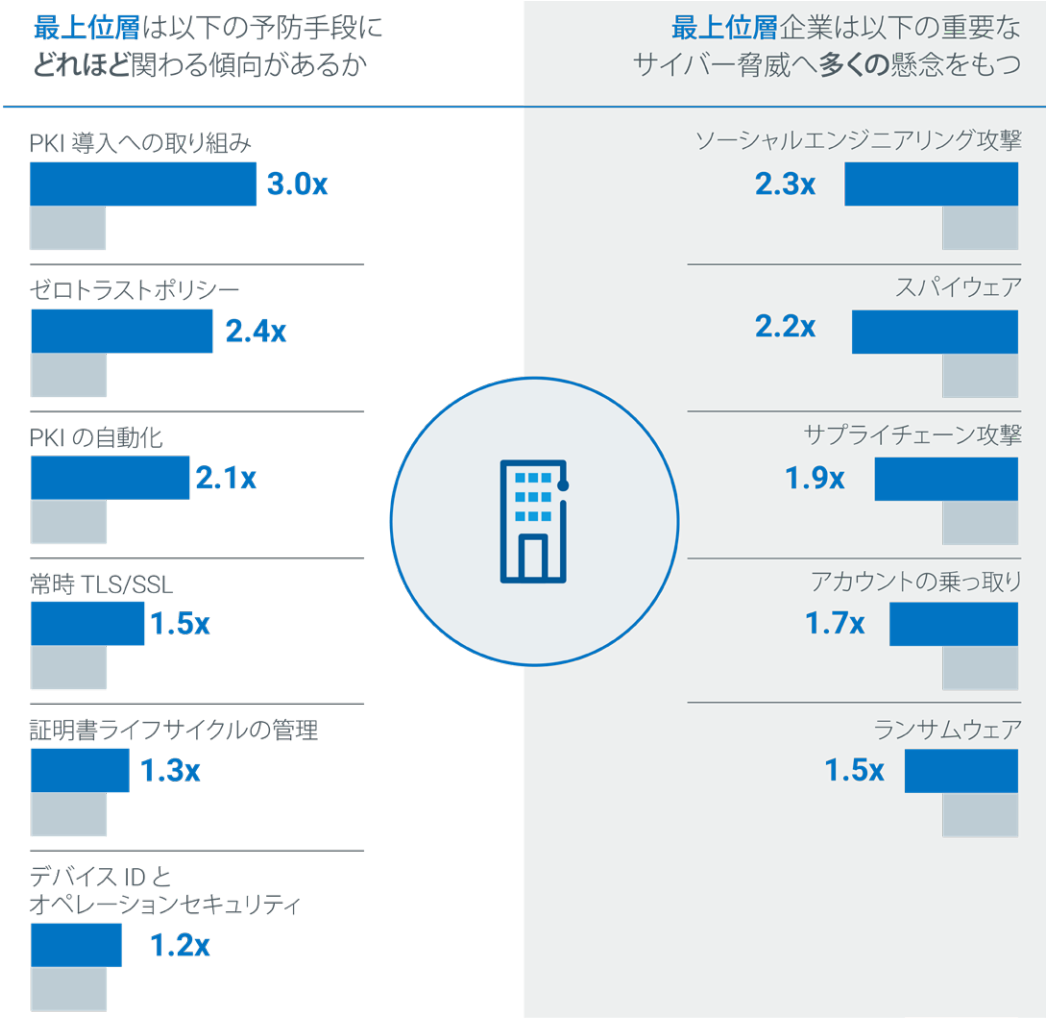
デジタルトラストについて、最上位層の企業は
最下位層の企業と比べて**はるかに**良い結果を出しています。



最上位層はなぜそこまで良いか

最上位層と最下位層の間にはさまざまな著しい違いがあり、デジタルトラストの結果に大きな差を作り出しています。

- 態度：最上位層では、顧客からの信頼を失うことが、その顧客を失うことにつながると信じる傾向が 4.5 倍高いです。彼らはまた、デジタルトラストが自社のブランド、売上、利幅に影響すると信じる傾向が高いです。加えて、最上位層では、パートナーへの信頼を無くした場合、パートナーを乗り換える傾向が 5.6 倍高いです。
- 早期の開始：先進層はデジタルトラストへの取り組みをさらに進めており、遅滞層よりもはるかに早期に取り組みを完了するでしょう。
- サイバー脅威への多くの懸念：最上位層はサイバー脅威をはるかに深刻に受け止めています。最上位層はサイバー脅威を懸念する傾向が 1.5 倍から 2.3 倍高いです。
- 一般的なサイバー予防手段にさらに関わる：最上位層は重要なサイバーセキュリティ予防手段に関わる傾向が最大で 3 倍高いです。



デジタルトラストは どこにあるべきか

企業組織のどこにデジタルトラストを配置するか決めることは、重要です。最上位層と最下位層の企業の間にあるこの問題について、明らかな意見の違いがあります。

最上位層は、CIO が IT 組織でのデジタルトラストを運営すべきだと述べています。一方、最下位層はこれに反対して、セキュリティオペレーションが運営すべきだと感じています。

これにより、セキュリティオペレーションやその役割を軽視しているのではありません。これらは組織にとって不可欠なことです。ただ、組織のより広範な技術的影響を CIO が見通している証とみなすべきです。そして、技術主導型組織の成功では、デジタルトラストがいかに重要であるかを認識するものとして捉えるべきです。この結果は最上位層企業のデジタルトラストへの戦略的アプローチに反映されています。

デジサートの見解

デジタルトラストを提供する世界有数のプロバイダーであるデジサートは、個人や企業がデジタル世界における操作に対し安全性を信頼して、オンラインで取引できるように取り組んでいます。デジサートは初期の頃からデジタルトラストに関わってきました。最上位層の「デジタルトラストの専門家」が実証した成功を模倣したい企業へのアドバイスは、以下の 5 点の実行を検討することです。

デジタルトラストを戦略的緊急課題とすること。これは、最上位層企業への明確な差別化要因の 1 つです。最上位層企業は、デジタルトラストがブランド、顧客ロイヤルティ、収益、利幅などの重要な営業成果に影響することを認識していました。

意志決定権を与えられた明確なリーダーがいる、組織の技術部門内にデジタルトラストオフィスを構築すること。

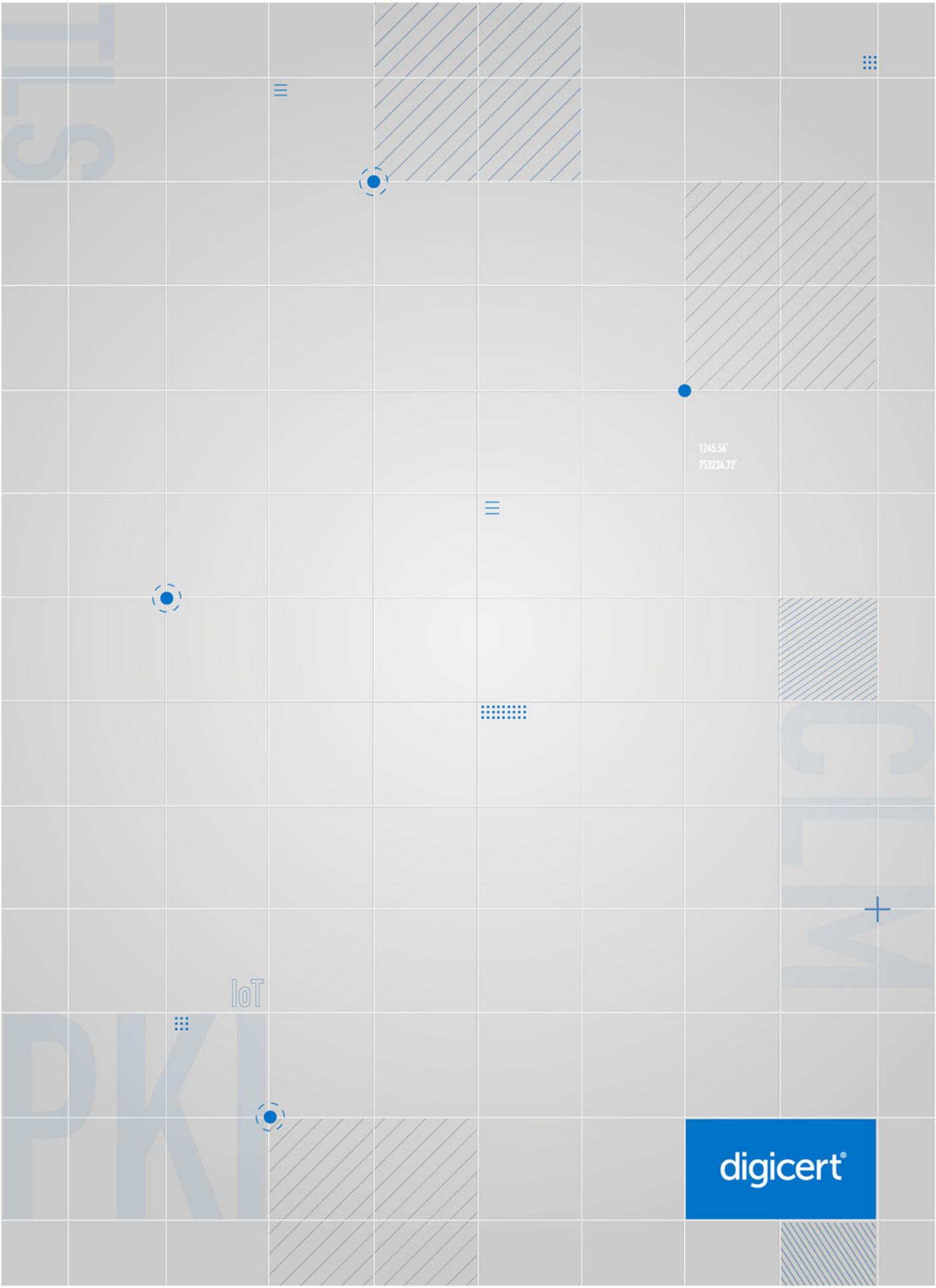
デジタルトラストの認知度がユーザー（消費者を含む）の間で高まっていることと、高いレベルのデジタルトラストを確保することで、営業の成功と評判が直接自分の能力と関連付られることを認識すること。

デジタルトラストを探求する上で専門家のサポートを確保すること。企業が挙げたデジタルトラストの課題の 1 つが、スタッフの専門知識不足でした。引き入れるパートナーが、デジタルトラストの構成要素にまたがる広範なポートフォリオを持ち、自社の組織全体に統合的なトラスト管理ソリューションを提供できること。

顧客はデジタルトラストに配慮することに注意。デジタルトラストによる顧客とのコミュニケーションに明確なラインを設定し、自身のデジタルトラストへの取り組みだけでなく、進捗も説明すること。

これは、Bain & Company[5] による調査結果と符号しています。その調査では、顧客の定着率が 5% 増加すると利益が 25% から 95% に増加することが示されています。顧客が企業への信頼を無くした場合にその企業から離れていこうとする傾向を考えると、デジタルトラストを最大限まで高めることが必須のアクティビティになるべきです。

[5]Prescription for Cutting Costs – Bain & Company


1245.56°
753234.72°
IoT
digicert®