Digital Architecture
Design Center

トラスト入門

2025年3月
デジタルアーキテクチャ・デザインセンター(DADC)

はじめに

■執筆の背景

近年、デジタル化や生成AIをはじめとするテクノロジーの進展、そしてグローバル化の進行により、様々な場面で「トラスト」の必要性が叫ばれるようになった。しかし、一口にトラストと言っても、話者がどのような意図でトラストという言葉を使っているのか、注意深く確認しないと誤解が生じるケースも増えてきている。そこで、トラストの基本的な考え方を整理して示すことにより、各ステークホルダーがトラストについての共通認識を持つことができ、議論がスムーズに、そしてより活発に行えるようになると考え、本書を執筆した。

■想定読者

本書は、トラストをこれから勉強しようとしている「トラスト初学者」を主な想定読者としている。

■本書で分かること(記載の範囲)

トラストの基本的な考え方について、馴染み深い旧来のトラストを例に理解し、その発展的な適用例としてサイバーフィジカルシステム(Cyber Physical System :CPS)を題材に、CPSにおいて検討すべきトラストの勘どころを掴むことができる。

■免責事項

本資料の内容は、完全性、正確性を保証するものではなく、今後予告なく大幅に加筆・修正する可能性がある。IPAは、本資料に記載されている情報により生じる損失または損害に対して、いかなる人物あるいは団体にも責任を負うものではない。

■改版履歴

日付	内容
2025/3/26	初版発行

目次

1.　トラストについて

1.1　トラストとは
1.2　トラストに影響を与える特性
1.3　検証可能な特性
1.4　特性の分類
1.5　信頼のよりどころ
1.6　トラストアンカー
1.7　デジタルトラスト
1.8　トラストサービス
1.9　トラストモデル

2.　Society5.0の実現に向けたトラスト

2.1　Society5.0におけるトラストの検討
2.2　3層構造モデルと6つの構成要素
2.3　3層構造モデルを用いたトラストの検討例
2.4　第1層におけるトラストの検討例
2.5　第2層におけるトラストの検討例
2.6　第3層におけるトラストの検討例
2.7　検証しない場合のリスクとトラストワージネス
2.8　各層における検証対象
補足　ゼロトラストセキュリティ

Appendix.

用語集
ISO/IEC TS 5723:2022
ISO/IEC 25012:2008

1.　トラストについて

1.1　トラストとは
1.2　トラストに影響を与える特性
1.3　検証可能な特性
1.4　特性の分類
1.5　信頼のよりどころ
1.6　トラストアンカー
1.7　デジタルトラスト
1.8　トラストサービス
1.9　トラストモデル

本章では、そもそもトラストとは何か(1.1)、そして相手とトラストを確立する際の判断材料となる特性(1.2～1.4)、また信頼のよりどころとトラストアンカー(1.5～1.6)について、例を交えながら解説する。また、デジタル空間上でのトラストという観点から、デジタルトラストとトラストサービス(1.7～1.8)にも触れる。

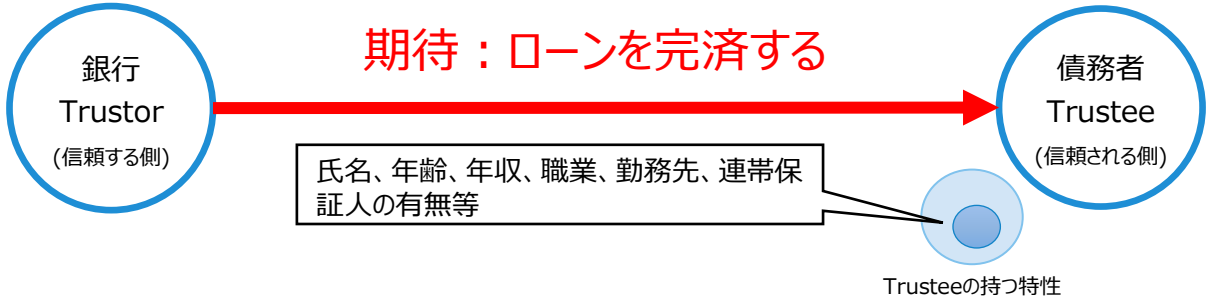
1.1　トラストとは

トラストという言葉の定義は様々存在するが、ISO/IEC 25010(JIS X25010)、また科学技術振興機構(JST)の研究開発戦略センター(CRDS)では以下の通り定義している。

・ISO/IEC 25010：**利用者又は他の利害関係者がもつ、製品又はシステムが意図したとおりに動作するという確信の度合い。**
出典：JISC 日本産業標準調査会(規格番号JIS X25010)
・JST CRDS:**相手が期待を裏切らないと思える状態。**
出典：デジタル社会における新たなトラスト形成｜戦略提案・報告書｜研究開発戦略センター（CRDS）

いずれの定義も、製品やシステム、相手に対しての期待があり、それが想定通り振る舞ってくれると思える度合い、またはその状態をトラストと定義している。本書では製品やシステムだけでなく、人や組織に対するトラストも議論の対象とするため、CRDSの定義した**「相手が期待を裏切らないと思える状態」**を基に解説を行う。

さて、トラストにおける「相手に期待すること」は、相手とトラストを確立したいと思っているTrustor(信頼する側)によって様々存在するはずである。住宅ローン審査を例に考えると、Trustorである銀行は、Trustee(信頼される側)である債務者に対し、ローンを完済することを期待するわけだが、Trusteeが毎月遅滞なくローンの返済を行い、予定通りに完済するかどうかを事前に確認することはできない。(未来を見ることができれば別だが。) そのため、TrustorはTrusteeがローンを完済できると思える**性質**や**特徴**をどれだけ有しているか、という観点で審査を行い、完済可能だと判断すればトラストが確立されローン契約が成立するが、その能力が無いと判断されれば契約は否決されることになる。

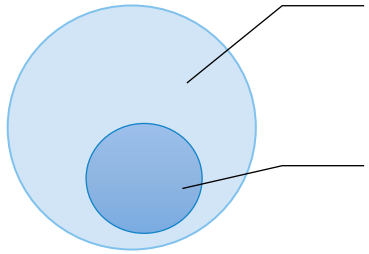


このように、相手が自分の期待に応えてくれるかどうか、トラストを確立してよい相手であるか、Trusteeが持つ性質や特徴を表す**特性**を総合的に判断し、Trustorの期待値(閾値)を超えている場合は信頼に足る対象であると見なし、トラストを確立するのである。トラストを確立するか否かの判断はTrustorの**主観**によって決まるものであり、当然トラストを確立する際の期待値(閾値)は、Trustorによって異なるはずである。特性については次ページ以降で解説を行う。

1.2　トラストに影響を与える特性

特性はTrusteeが備えていると主張する「性質・特徴」のようなもので、TrusteeとTrustorのトラストに影響を与えるものである。下図では、特性を濃い円と薄い円で表しているが、濃い円はTrustorが「計測/観測/検証可能な特性」として表している。本書では、Trusteeがある特性を備えていることの検証方法をTrustorが利用できるとき、Trusteeはその特性に対してトラストワージネス(Trustworthiness)を備えているという。Trusteeが備えることが望ましいトラストワージネスは、社会情勢やステークホルダの要求に基づいて様々なものが考えられる。

Trustworthiness：ability to meet stakeholders' expectations in a verifiable way.
出典：ISO/IEC TS 5723:2022



Trusteeの持つ特性

薄い円：Trusteeが備えていると主張する特性の中で、実際に備えているかどうかをTrustorが直接検証できない領域を示す。この範囲が広い場合、相手の主張を根拠なく信頼しなければならない部分が大きくなるため、Trustorの期待が裏切られる可能性は高くなる。
このように、検証できない特性を元に確立したトラストは、暗黙的なトラスト(Implicit Trust)と呼ばれる。

濃い円：Trusteeが備える特性の中で、Trustorが検証(計測、観測も含む)する方法が提示されている領域を示す。検証の結果、Trusteeの主張した通りの特性を備えている事を確認することができれば、Trustorの期待が裏切られる可能性は低くなる。
このように、特性を検証した上で確立したトラストは、明示的なトラスト(Explicit Trust)と呼ばれる。

相手とトラストを確立する際のこのようなアプローチは、Trusted Webのホワイトペーパーにて詳しく検討されているため、参照のこと。

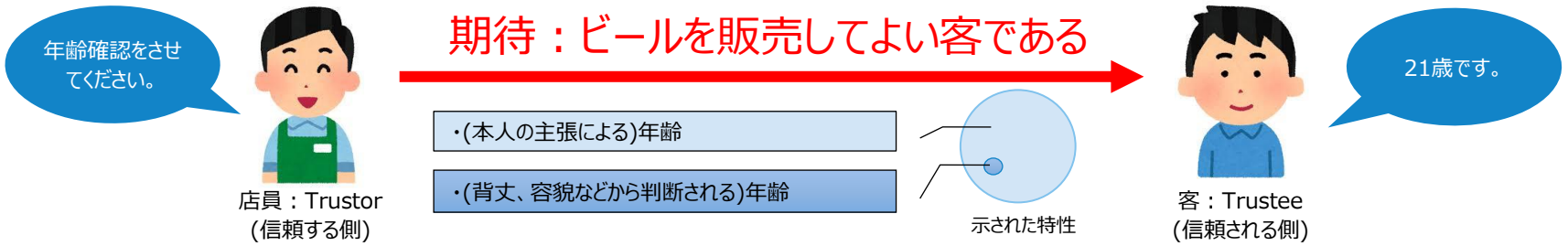
薄い円に含まれる特性は、相手の言い分を根拠なく信頼しなくてはならない部分であり、濃い円に含まれる特性は自分も確認したので根拠をもって信頼できる、といえる範囲である。尚、トラストワージネスを備えていれば確実に信頼できるという訳ではなく、どの程度信頼できるのか、という信頼の度合い(レベル感)が存在する。
本人確認を例とすれば、あるレベルでは運転免許証の券面情報の確認、あるレベルではマイナンバーカードの電子証明書の確認、といった具合である。この信頼度の度合いについては、「1.5 信頼のよりどころ」で解説する。

補足：本書では今後、トラスト、トラストワージネスを以下の定義で使用する。
・トラスト(Trust)：**相手が期待を裏切らないと思える状態**
　ー使い方：トラストを確立する、トラストを確保する、トラストを形成する、トラストを担保する
・トラストワージネス(Trustworthiness)：**相手の期待に対して検証可能な方法で応える能力**
　ー使い方： トラストワージネスを備える、トラストワージネスを示す

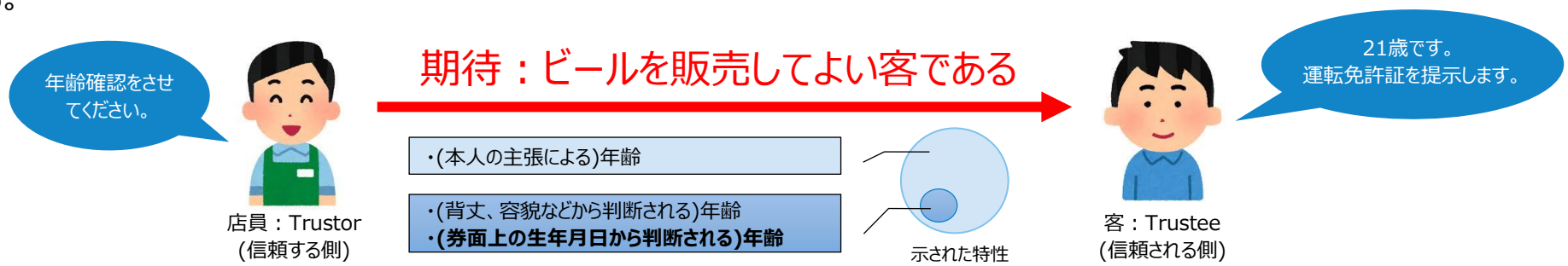
参照：ホワイトペーパー・関連資料 | Trusted Web

1.3　検証可能な特性

検証可能な特性に関する例として、コンビニでビールを販売する例を考える。この例では、**「ビールを販売してよい客である」**というものを店員の期待として設定する。店員はビールを販売してよい客であることを確認するため、1つの手段として年齢を確認するが、「21歳です」という口頭での回答だけで良しとするケースはほとんどないはずである。それは客の主張を根拠なく(検証しないで)信頼することになるからである。この状態でトラストを確立してしまうと、未成年者に対してビールを販売してしまう可能性が高まり、そのリスクを店側が負うことになる。



一方で、客から運転免許証が提示された場合、券面上の顔写真と生年月日を確認することによって、客が年齢を偽りなく申告していることを確認(検証)することができるため、20歳以上であればその事実を踏まえてビールを販売することができるし、20歳未満であれば販売せず、未成年者に対してビールを販売してしまうリスクを回避することができる。



このように、検証可能な範囲が広がれば、初対面の相手でも**「相手が期待を裏切らないと思える状態＝トラスト」**を容易に確立することが可能となり、他者との円滑な取り引きを行うことができるようになるため、ビジネスの発展にも役立たせることができるとされている。尚、この例では年齢確認という目的のため運転免許証を提示しているが、運転免許証には名前や住所等、年齢確認に不要な情報も掲載されており、本来提示不要なTrusteeの個人情報をTrustorに提示することになる点は、留意が必要である。

補足：背丈や容貌などはTrusteeから意図的に示されるものではないが、Trustorが観測可能な特性であるため、検証可能な特性の一つとして示している。この特性からビールを販売してもよい客であるかを判断できるケースもあるが(むしろその方が多いかもしれない)今回の例ではそれだけではビールを販売してよい客か判断ができなかった場合を示している。

1.4　特性の分類(1/3)

ここまで特性について解説してきたが、前述のCRDSの報告書によると、特性はどのような側面に着目するかによって、「対象真正性」、「内容真実性」、「振る舞い予想・対応可能性」の3通りに整理できるとされている。(この分類に当てはまらないケースも存在する。)また、それぞれの側面から示される特性が、同じ対象を示しているのか、紐づきの確認をすることも重要な観点となる。例えば本人確認を行うために運転免許証の提示を受けた場合、その運転免許証が本当にその人に発行されたものなのか、他人の運転免許証を提示していないか、という観点の確認が必要である。

紐付きの確認

3側面	どのような側面か
対象真正性	**本人・本物であるか？** 人であれば相手が本人なのか、物であれば本物なのかを示す特性。ブランド品の真贋問題などは対象真正性の問題となる。また、電子データや紙媒体の情報における対象真正性は、オリジナルの情報から改ざんされていないか、という観点となる。
内容真実性	**内容が事実・真実であるか？** 示された内容が本当に正しいのかを示す特性。その人の言っていることは本当なのか、商品につけられたレビュー評価、コメントの内容は正しいのか、といった観点である。対象真正性が正/偽の2値なのに対して、内容真実性はある程度のグラデーションがあると言われている。
振る舞い予想 対応可能性	**対象の振る舞いに対して想定・対応できるか？** 相手が期待通りに振る舞ってくれるかどうかを示す側面である。対応可能性についてはイメージがつきにくいかもしれないが、例えば相手が期待通り振る舞ってくれなった場合、そのリカバリや補償の対応を行う能力を有しているか、という観点である。(契約違反時の罰則、連帯保証人の有無など)

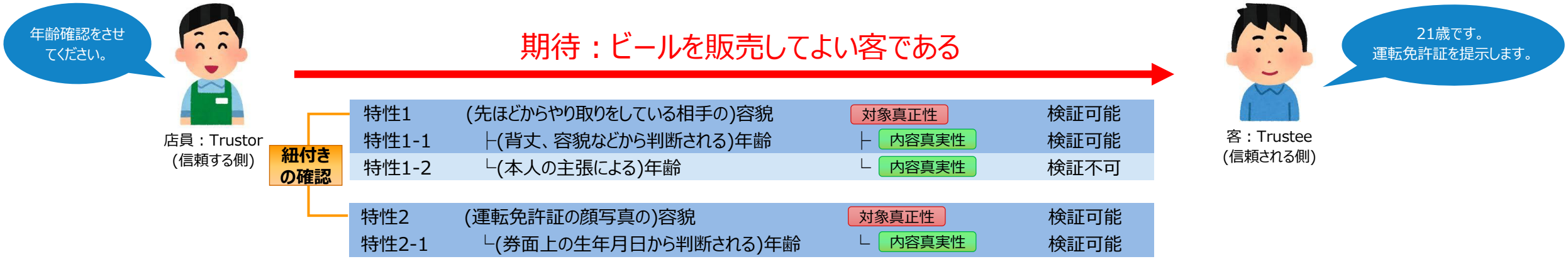
これらの3側面を多面的・複合的に捉えたうえで、トラストを確立してよい相手かどうか、総合的に判断することになる。

参照：デジタル社会における新たなトラスト形成｜戦略提案・報告書｜研究開発戦略センター（CRDS）（jst.go.jp)

1.4　特性の分類(2/3)

前スライドで示した3つの側面を、先のコンビニでビールを販売するという例に照らし合わせると、以下のように整理ができる。
21歳であるという本人の主張は、ビールを販売してよい客であるか(20歳以上であるか)を判断するための、Trustorが検証することのできない「内容真実性」に関する特性となる。一方、運転免許証の券面上の顔写真は、提示された免許証が、目の前にいる客に払い出されたものである、という「対象真正性」を示す特性であり、券面上の生年月日はその人物を説明する情報として、年齢の「内容真実性」に関する特性であると言える。

	3側面	どのような側面に関するトラストか
紐付きの確認	対象真正性	本人・本物であるか？
	内容真実性	内容が事実・真実であるか？
	振る舞い予想・対応可能性	対象の振る舞いに対して想定・対応できるか？

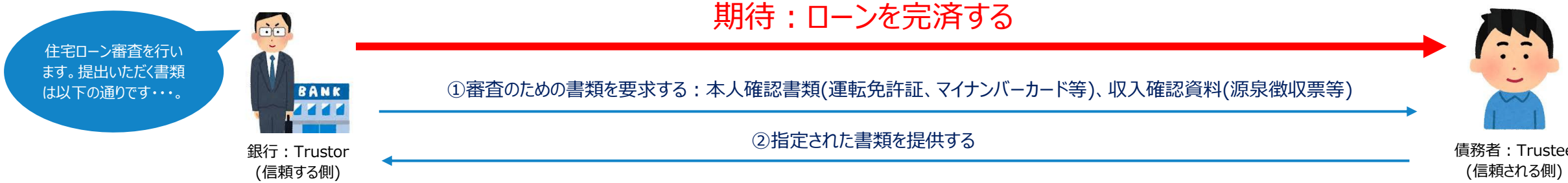


この例では目の前にいる客の容貌と運転免許証の顔写真を照合し、特性1と特性2が紐づいていることを確認している。このように、同一の対象を示す特性が複数の情報源から提示された場合は、それらの紐付きを確認することが重要となってくる。

参照：デジタル社会における新たなトラスト形成｜戦略提案・報告書｜研究開発戦略センター（CRDS）（jst.go.jp)

1.4　特性の分類(3/3)

特性に関する3つの側面について、もう1つ例をあげて解説する。本章の冒頭でも例示した住宅ローン審査を行う場合を考える。Trustorである銀行は、Trusteeである債務者に対して「ローンを完済する」ことを期待するが、未来を知ることができない以上、その期待が実現されるであろうことを事前に確認することは不可能である。そのため、期待に応えるだけの特性を債務者は有しているか、という観点で審査を行う。



Trustorの「ローンを完済する」という期待において、Trustorが直接的に求めるトラストの側面は「対象真正性」と「振る舞い予想・対応可能性」の2点と考えられる。「内容真実性」はTrusteeが提示する特性が本当に正しいかを検証するために、重要視される観点となる。

期待	期待に対して重要視される側面	検証に資する特性の例		特性を示す例			発行者
ローンを完済する	対象真正性	氏名	内容真実性	運転免許証、マイナンバーカード	対象真正性	紐付きの確認	公的機関
		住所	内容真実性				
		生年月日	内容真実性				
	振る舞い予想 対応可能性	年収	内容真実性	源泉徴収票	対象真正性		民間企業等
		勤務先	内容真実性				
		健康状態	内容真実性	健康状態告知書	対象真正性		本人(債務者)

免許証やマイナンバーカードのように、対象真正性が確認できれば、同時に内容真実性も担保できるケースもあるが、健康状態告知書のように、書類は本人が書いた本物であっても、内容に嘘偽りが無いかまでは担保できないケースも存在する。これはその書類を誰がどのような確認を経て発行したか(お墨付きを与えたか)、また虚偽記載が明らかになった際にどのようなペナルティが課されるのか、などによって信頼の度合いが変わってくるからである。信頼の度合いはTrustorの主観や社会的合意等で決まるものであり、何を信頼のよりどころとして置いているかが重要な観点となってくる。この信頼のよりどころについては次スライドで解説を行う。

補足：生年月日は「対象真正性」(本人かどうか)と「振る舞い予想・対応可能性」(返済期間の妥当性)の判断に利用されることがあるため、この例では両方の側面を持つ整理としている。

1.5　信頼のよりどころ

TrustorとTrusteeがトラストを確立するために示す特性について、何を信頼のよりどころとして相手に提示するかは、ユースケースやTrustorの主観、社会情勢によっても変わってくる。以下は人、組織、物を例に、現代社会において特性を示す手段として利用されている例の一部を示す。

対象 / 3側面	人	組織	物
対象真正性	**容貌**、サイン、身分証、実印、生体認証など	代表者のサイン、法人実印など	バーコード、QRコード、ホログラム、刻印、鑑定書など
内容真実性	資格証明書、社員証・学生証、運転免許証、**住民票**など	**有価証券報告書**、法人登記情報など	鑑定書、認定証など
振る舞い予想・対応可能性	**口約束**、資格証明書、運転免許証、法律・憲法など	取引実績、適合性認証、企業認定、契約書、法律・憲法など	取扱説明書、保証書、仕様書、**適合性認証**など

以上のように、特性を示す手段は様々存在するわけだが、手段によってどれだけ信頼できるのか、という**信頼の度合い**は異なる。それは特性を示す各手段の「信頼のよりどころ」が何なのか、という点が異なるからである。上記表で示したいくつかの手段(太字)について、信頼のよりどころとなっているものを以下に例示する。

確認手段	信頼のよりどころ	信頼の度合い
容貌	TrustorのTrusteeに関する記憶、経験。または証明写真等との照合結果など。	過去にその人物と会っている場合、顔や容貌を記憶しているため、本人性確認の手段として利用できる。また写真と照合することで本人性確認を行うこともできる。写真と照合する場合は、写真の内容真実性(改ざんされていないかなど)に関わる観点も考慮が必要となる。いずれも人の記憶や主観に頼るところがあるため曖昧さは残るが、一般的によく利用されている。
適合性認証	独立した第三者機関による認証。	第三者機関の独立性、専門性、透明性、規格の遵守、継続的な監査などの様々な要因により、信頼の度合いが決まってくる。第三者による客観的な評価が期待できるため、一般的に信頼度は高いとされるが、どのような認定を受けた機関なのか、確認が必要。
有価証券報告書	有資格者による監査、虚偽記載時の法的罰則や社会的信頼の失墜など。	金融商品取引法に基づいて作成され、虚偽記載があれば法的な罰則が科される可能性がある。また監査法人や公認会計士などによる監査も義務付けられているため、一般的に信頼度は高いとされる。
住民票	公的機関が発行。	住民票は市区町村の役所が発行する公的な文書であり、法的な効力を持つため、信頼度は高いとされる。但し、公的機関がどの国でも常に信頼できるとは限らず、政情不安や法制度の健全性などによって左右される場合があることは、留意が必要である。
口約束	当事者間の信頼関係。	長年の付き合いや強い信頼関係がある場合、口約束でも十分に信頼されることがあるが、書面に残らないため法的な証明も難しく、契約書などと比べ信頼度は低い。

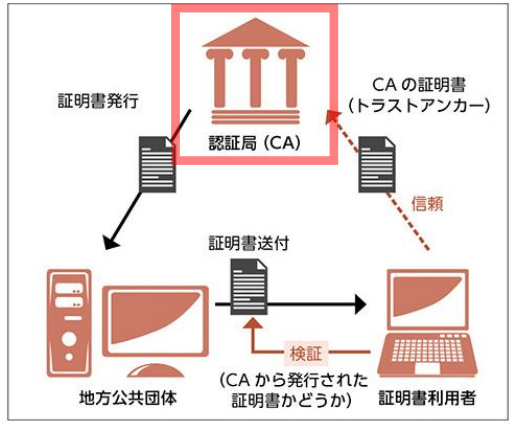
信頼の度合いが高ければ良く、低いと悪いという事はない。**ユースケースによって最適なものを選択**することが重要である。また、運転免許証のように、身分の証明(対象真正性)、年齢の証明(内容真実性)、運転技術の証明、事故発生時の適切な対応(振る舞い予想、対応可能性)、といったように、同じ手段でも検証の観点によって期待される側面が異なる場合があることはご留意いただきたい。

1.6　トラストアンカー(1/3)

信頼のよりどころに近しい考え方として、**トラストアンカー(Trust Anchor)**と呼ばれるものがある。トラストアンカーとは、一般的に公開鍵基盤(Public Key Infrastructure ：PKI)における最後の信頼の基点(Trust Point)となるルート証明書やルート認証局を意味する。一方で、近年ではトラストを確立したいと考えているステークホルダが抱く期待に対して、この人(人とは限らない)が「問題無い」と言っているのだから大丈夫、と**ステークホルダ間(トラストを確立したいと考えている人々)で合意形成ができている対象**(証明書そのものや、証明書の発行者、またはその認定機関等)をトラストアンカーと呼称するケースが増えてきている。トラストアンカーの使われ方について、以下に例を示す。

従来のトラストアンカーの意味合い

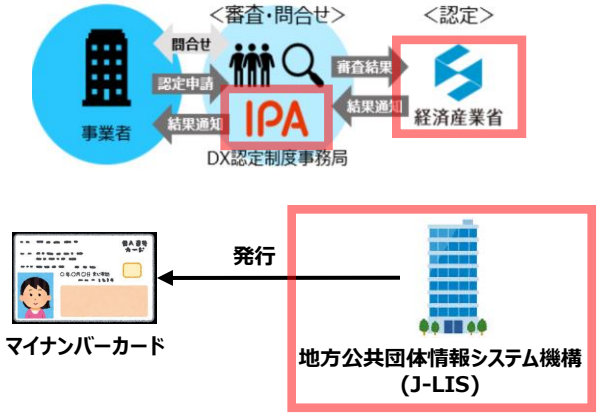
トラストアンカーの従来通りの使われ方。公開鍵基盤におけるルート証明書、またはルート証明書を発行するルート認証局をトラストアンカーと呼称するケース。



出典：LGWAN総合行政ネットワーク　VOL.214　LGPKIの仕組みについて（後編）
月刊J-LIS 2020年8月号｜地方公共団体情報システム機構

拡張されたトラストアンカーの意味合い

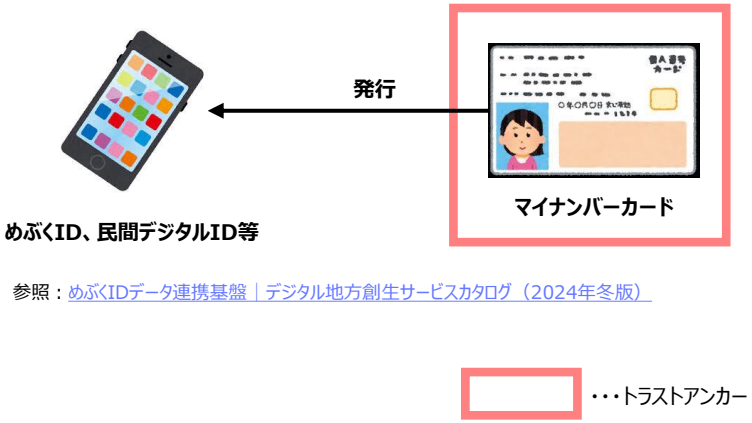
信頼の基点を辿った先の最後の基点、という従来の意味合いからの拡張として、証明書等の発行業務を担っている組織、またはその組織にその業務を行うことを認めた(認定した)組織をトラストアンカーと呼称するケース。



参照：DX認定制度のご案内｜社会・産業のデジタル変革｜IPA 独立行政法人 情報処理推進機構
公的個人認証サービス（JPKI）｜デジタル庁

表現上の分かりやすさから使われるトラストアンカーの意味合い

表現上の分かりやすさから、信頼できる対象そのものをトラストアンカーと呼称するケース。近年ではこのような使われ方も増えてきていることに留意が必要。

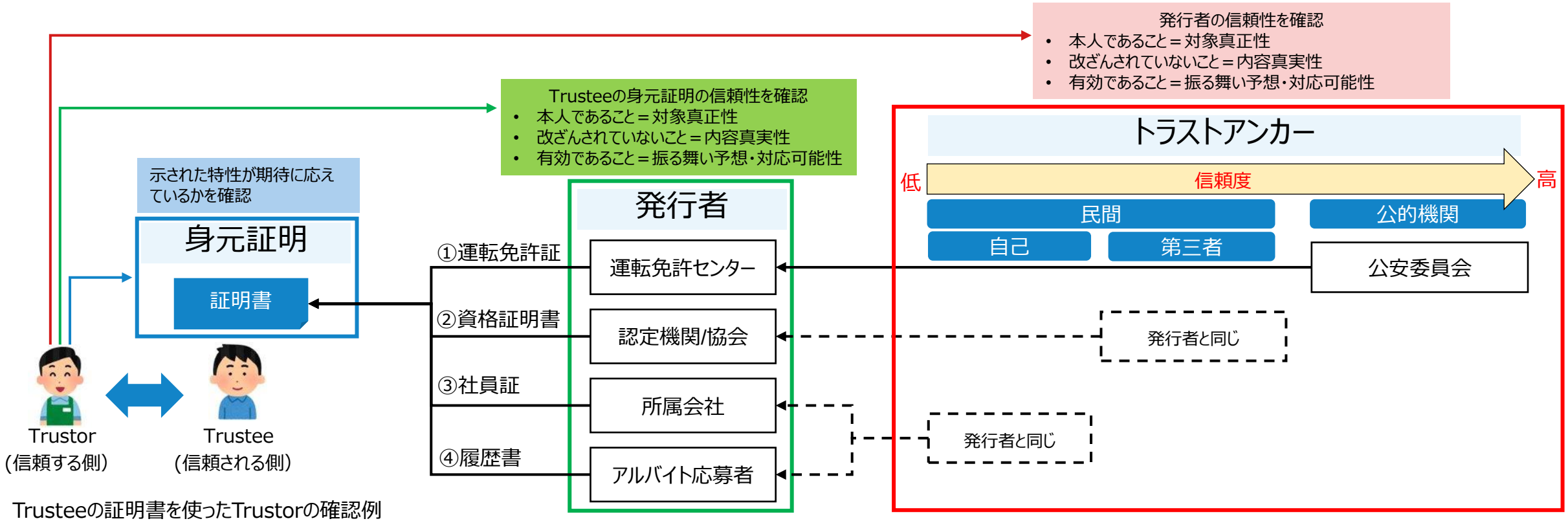


参照：めぶくIDデータ連携基盤｜デジタル地方創生サービスカタログ（2024年冬版）

以上のように、様々な場面でトラストアンカーという言葉が使われているため、どのような意図で使われているかは注意深く確認する必要がある。尚、本書におけるトラストアンカーの意味合いは、「拡張されたトラストアンカーの意味合い」として使用する。

1.6　トラストアンカー(2/3)

トラストアンカーとなる候補として、一般的には「民間(自己)」、「民間(第三者)」、および「公的機関」が存在する。特性の期待に法令等が含まれない場合は民間のトラストアンカーで充足するケースもあるが、法令等が含まれる場合は、信頼度の高い公的機関をトラストアンカーとすることの検討が必要である。以下は身元証明を例に、ユースケース毎のトラストアンカーの例を示す。



Trusteeの証明書を使ったTrustorの確認例

特性の期待	No	証明書	身元証明
お酒を販売してよい客	①	運転免許証	運転免許証の「顔写真・生年月日」を確認し20歳以上であることを確認。
英語が話せること	②	資格証明書(英語検定等)	資格証明書の「氏名・資格」を確認し特定の能力(英語を話せる能力)を有していることを確認。
取引先の社員	③	社員証	社員証の「顔写真・氏名・会社名」を確認し取引先の社員であることを確認。
アルバイト募集	④	履歴書	履歴書の「顔写真・氏名・住所・生年月日」を確認し応募者本人であることを確認。

1.6　トラストアンカー(3/3)

その他にも、関係者の期待に応じて様々なトラストアンカーがあるので紹介する。

1.監査機関登録の要求事項を満たす**クラウドサービス**
　　例：「政府情報システムのためのセキュリティ評価制度(Information system Security Management and Assessment Program)」
　　通称 ISMAPの登録事業者サービス(ISMAPクラウドサービスリスト - ISMAPポータル)

2.信頼されたデータソースになる公的基礎情報**データベース**
　　例：ベース・レジストリ(デジタル庁にて整備中)

3.適合性評価機関に認定された**トラストサービス**
　　例：EUにおける認定されたトラストサービスプロバイダー(TSP)のリスト(eIDAS Dashboard)

トラストアンカーを定めるメリットはいくつかあるが、代表的なものを以下に示す。

メリット	説明
トラスト水準の統一	トラストを確立するための水準を統一することができるため、ステークホルダ間の信頼の度合いに整合性が生まれる。
コミュニティの拡大	トラストの基準が定まることにより、コミュニティへの参加条件などが明確になり、コミュニティの拡大に寄与する。
客観性の向上	誰が評価しても同一の基準に従い客観的に判断できるため、主観的な判断の影響を受けにくくなる。

参照
1.ISMAP「政府情報システムのためのセキュリティ評価制度」
2.デジタル庁「ベース・レジストリ」
3.Data Spaces Support Center「Blueprint v1.5 Trust Framework」

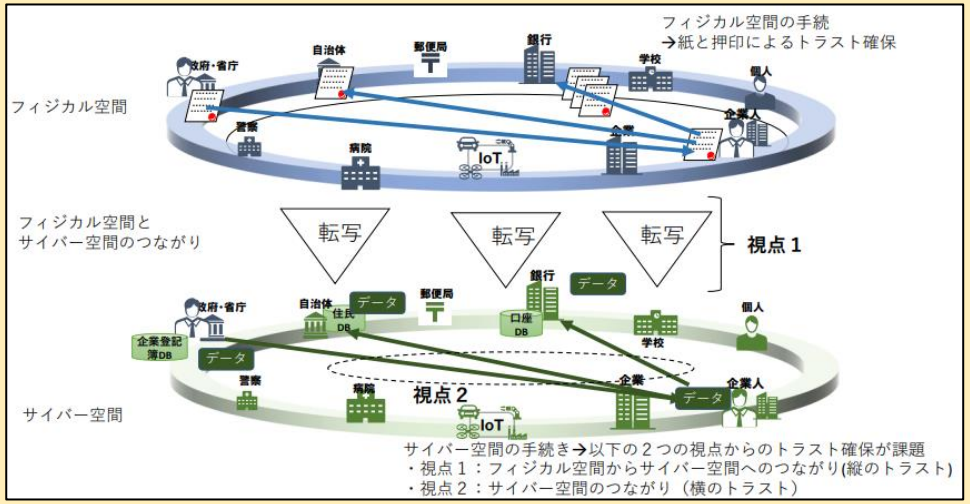
1.7　デジタルトラスト

ここまで信頼のよりどころやトラストアンカーについて解説してきたが、昨今ではデジタル社会の広がりにより、顔が見える人間関係やルール、従来から利用されてきた信頼のよりどころだけでは、トラストを確立できないケースが増えてきている。CRDSの報告書では以下三つをその要因として挙げている。

第一の要因は、インターネットを介した商取引やSNS（Social Networking Service）などに見られるように、バーチャルな空間にも人間関係が広がったことである。
第二の要因は、人工知能（Artificial Intelligence: AI）などの、複雑でブラックボックスとも言われる技術を用いたシステムへの依存が高まったことである。
第三の要因は、AI技術によるフェイク画像・動画・音声の生成や、アカウントのなりすましなど、「だます技術」が高度化していることである。

出典：デジタル社会における新たなトラスト形成｜戦略提案・報告書｜研究開発戦略センター（CRDS）（jst.go.jp）

そこで、近年ではデジタル空間におけるトラスト、いわゆる**デジタルトラスト**の担保が求められるようになってきている。一般社団法人デジタルトラスト協議会(JDTF)では、デジタルトラストを**「デジタル空間において、人・組織・モノ・データ・プロシージャ・システムが、ステークホルダーからの信頼を得られている状態」**と定義しており、デジタル空間(サイバー空間)上でのトラスト確保において、要求される機能や仕組みと、それらを実現する際の課題を2つの視点から提起している。



出典： JDTF-RMWGホワイトペーパーVer1.0s.pdf

視点1：サイバー空間とフィジカル空間の境界において、適切かつ正確に情報が転写されることの担保
- 1-1 フィジカル空間の人・組織・モノに対するサイバー空間の ID 発行と、ID 発行時のフィジカル空間における実在性確認。
- 1-2 フィジカル空間の手続きがサイバー空間のシステムにより正しく実現できていることの確認。
- 1-3 サイバー空間の ID とフィジカル空間の人・組織・モノの対応付け（認証など）。
- 1-4 フィジカル空間の手続きの厳格さに応じて求められる、上記1-1～1-3の確認や対応付けに関するルールおよび制度。

視点2：データの流通・管理や適切な編集・加工を行うために必要となる対策や仕組みの構築
- 2-1 サイバー空間で行われる手続きやデータに関する発行元、時刻、意思確認。
- 2-2 フィジカル空間で同一の人・組織・モノに対応するサイバー空間のID同士の紐づけ。
- 2-3 フィジカル空間の手続きの厳格さに応じて求められる、上記2-1、2-2の確認や紐づけに関するルールおよび制度。

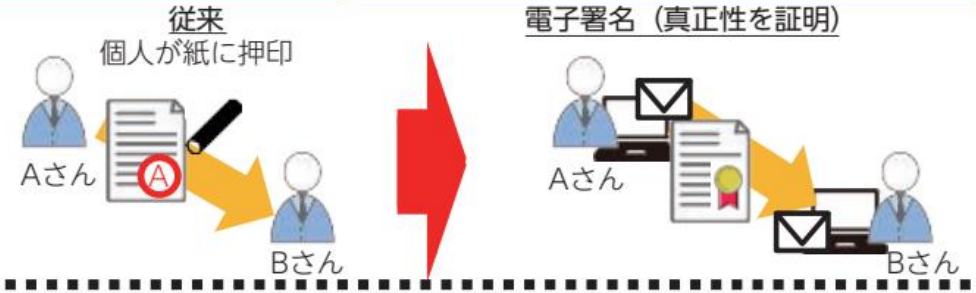
デジタルトラストを確立するための手段、主に視点2における課題の解決策として、いわゆる**トラストサービス**と呼ばれるものが存在する。次スライドでは代表的なトラストサービスについて紹介する。

1.8　トラストサービス

トラストサービスの代表的な例を以下に示す。
尚、eシールに関しては本書執筆時点において、認定制度の実現に向けた取り組みが進んでいる。

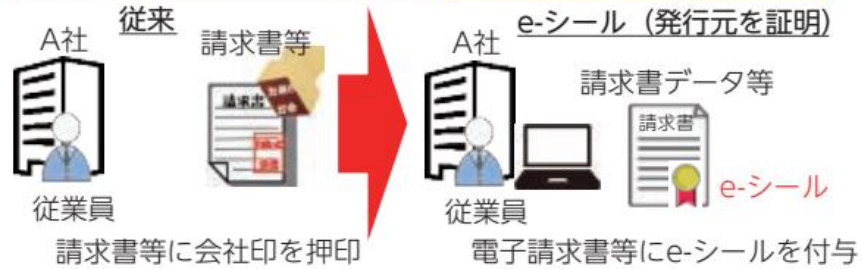
・電子署名（電子データの作成者を示す目的で行われる暗号化等の措置であって、電子署名が付されて以降、当該電子データが改変されていないことを確認可能とする仕組み）

国の制度有り（電子署名法）　一定の基準を満たす認証業務を主務大臣が認定



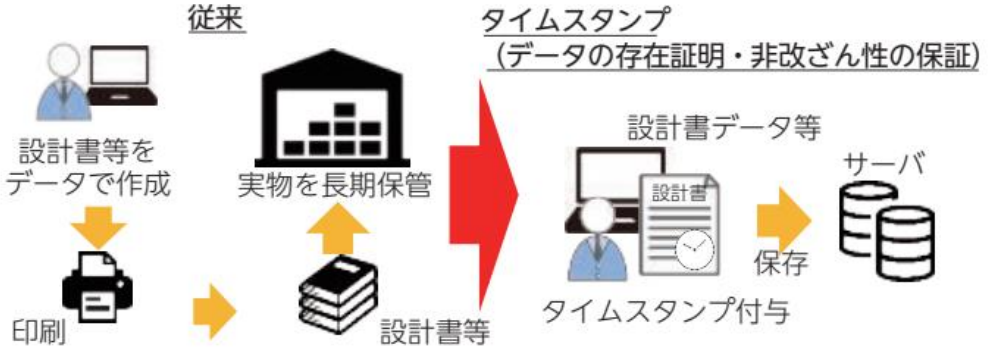
・eシール（電子データの発行元の組織等を示す目的で付与されるデータであり、付与されて以降、当該電子データが改変されていないことを確認可能とする仕組み）

国の指針あり（eシールに係る指針）　技術上、運用上の基準を整理

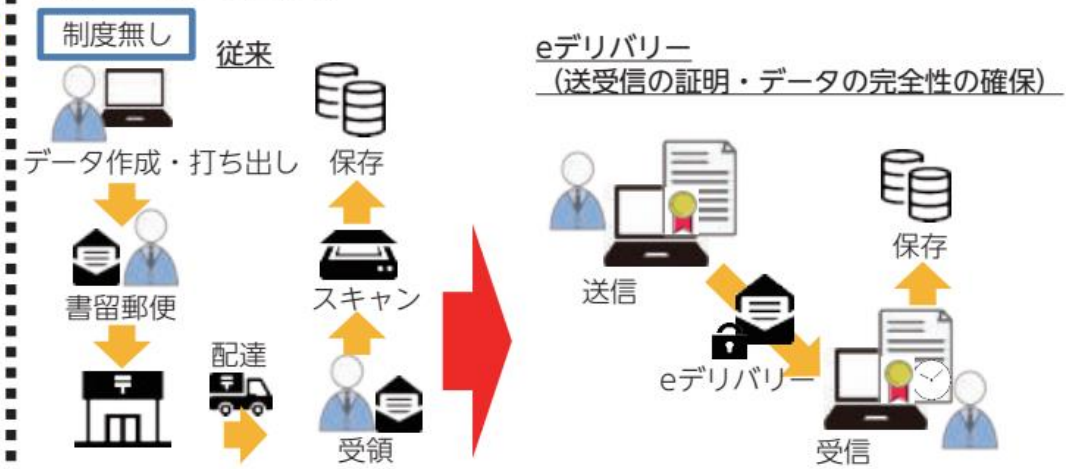


・タイムスタンプ（電子データがある時刻に存在し、その時刻以降に当該電子データが改変されていないことを証明する仕組み）

国の制度有り（総務省告示）　一定の基準を満たす時刻認証業務を総務大臣が認定



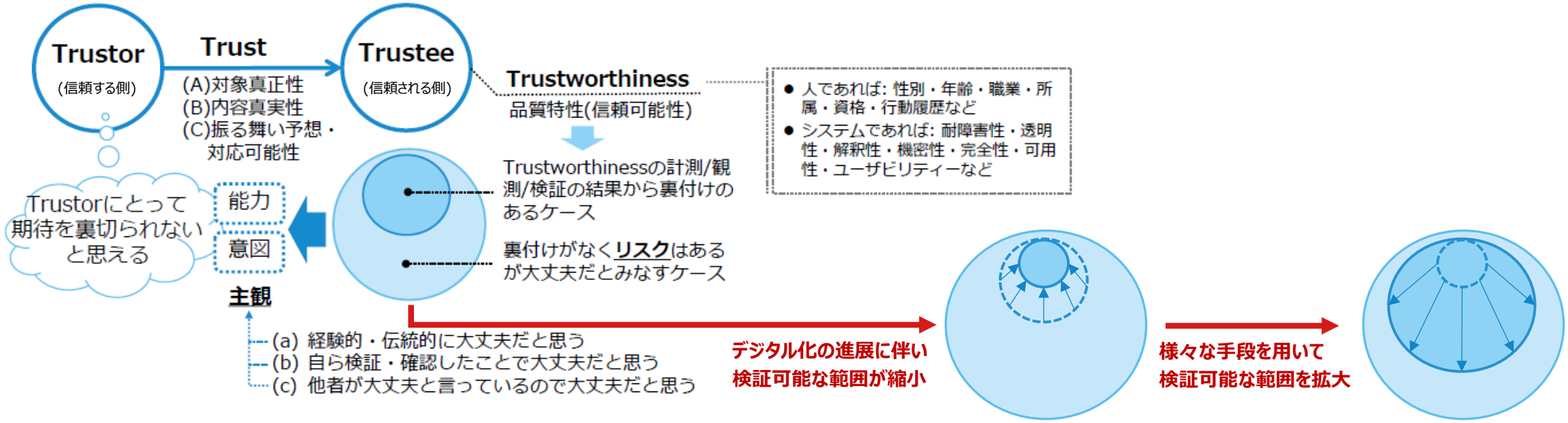
・eデリバリー（電子データの送信・受信の証明や送受信されるデータの完全性の確保を実現する仕組み）



出典：令和6年版情報通信白書
参照：「eシールに係る認定制度の関係規程策定のための有識者会議取りまとめ（案）」及び「eシールに係る認証業務の認定に関する規程（案）」に対する意見募集

1.9　トラストモデル

本章で解説してきた内容は、CRDSの報告書によると以下に示すトラストのモデルで表すことができる。
Trustor(信頼する側)は、期待が裏切られないと思える状態を確立するために、Trustee(信頼される側)から提示される特性を確認し、相手とトラストを確立するかどうかを判断する。Trusteeから提示される特性は、検証できるものと検証できないものが存在する。検証できない特性が多ければ、その分相手の主張を根拠なく信じなくてはならず、その範囲が広ければ広い程、期待が裏切られる可能性が高くなり、トラストを確立した場合のリスクも大きくなる。



出典：デジタル社会における新たなトラスト形成｜戦略提案・報告書｜研究開発戦略センター（CRDS)を元にDADCが作成

近年ではデジタル化の進展に伴い、従来であれば対面での確認等により検証できたはずの範囲(濃い円の範囲)が縮小し、相手を裏付けなく信頼しなくてはならないケースが多くなってきている。デジタル環境で情報(データ)をやり取りする際に、取引相手やデータを検証する手段がないと、データに対する信頼が低下し、円滑な取引が損なわれるという課題が生じる。この状況を改善するため、検証可能な濃い円の範囲、つまり内側の円を拡大するために、認定・認証制度などの制度的対策、そしてトラストサービスに代表される技術的対策を複合的に活用することにより、トラストを確立していくことが重要であるといえる。

2.　Society5.0の実現に向けたトラスト

2.1　Society5.0におけるトラストの検討
2.2　3層構造モデルと6つの構成要素
2.3　3層構造モデルを用いたトラストの検討例
2.4　第1層におけるトラストの検討例
2.5　第2層におけるトラストの検討例
2.6　第3層におけるトラストの検討例
2.7　検証しない場合のリスクとトラストワージネス
2.8　各層における検証対象
補足　ゼロトラストセキュリティ

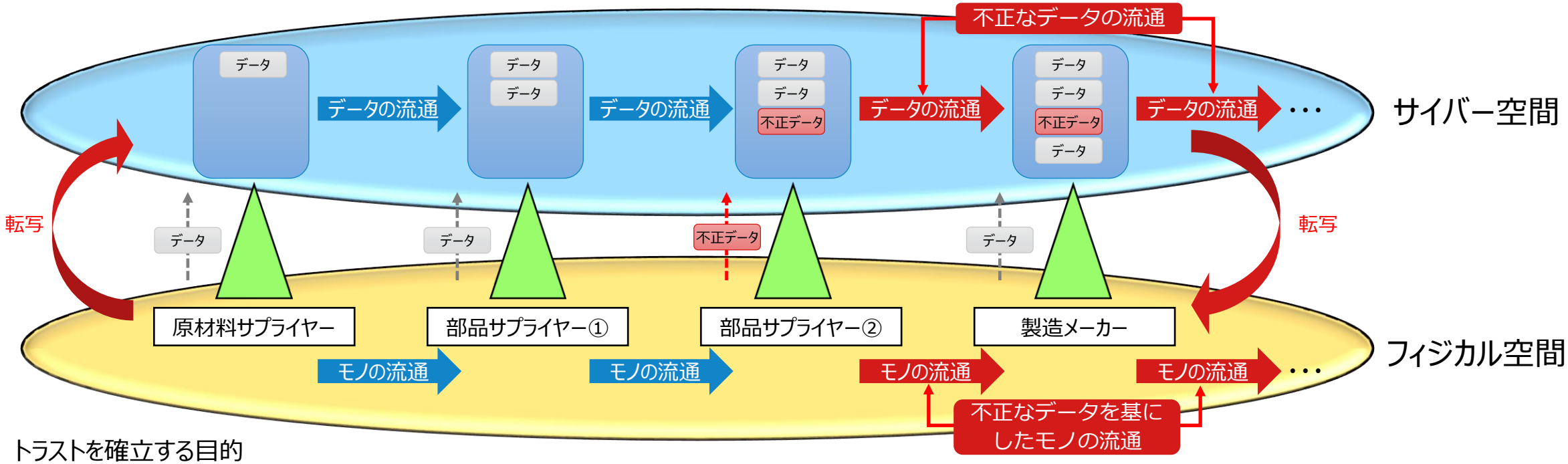
2章では、CPSF(Cyber Physical Security Framework)で示されている3層構造モデルと6つの構成要素を利用し、CPSにおけるトラスト検討のアプローチ方法を示し、(2.1～2.3)その具体的な検討例を解説する。(2.4～2.8)

2.1　Society5.0におけるトラストの検討

1章ではトラストの基本的な考え方についての解説を行ってきたが、2章ではその考え方を踏まえた上で、**Society5.0において実現していくべきサイバー空間とフィジカル空間を高度に融合させたシステム(Cyber Physical System :CPS)**を例にトラストの確立について検討する。

■　背景

CPSを活用することで、経済発展と社会的課題の解決を両立させる人間中心の社会が実現できるとされている。多様なステークホルダーの合意形成を図り、各分野間の整合がとれた社会の実現においては、トラストの重要性が増している。特に、新たなビジネス構造が構築される中で、フィジカル空間における従来のトラストだけではなく、サイバー空間でやり取りされるデータの信頼性に着目したトラストも重要であると考えられる。
サプライチェーンにおいてトラストが確立されていない場合のリスクとして、一部の企業が作成した不正なデータがサプライチェーン上に流通してしまい、データの利活用を阻害するだけでなく、不正なデータに基づいた不適切な部品や製品の検査、製造が行われ、サプライチェーン全体の信頼が失われてしまう、などが挙げられる。



■　トラストを確立する目的

ビジネスに関与するステークホルダ間でトラストを確立することで、データを安心・安全に流通することが可能となり、フィジカル空間における様々なやりとりをサイバー空間において円滑に行ったり、データに基づく価値の創出活動を支えたりすることができる。

Digital Architecture Design Center　参照：内閣府「Society 5.0 - 科学技術政策」

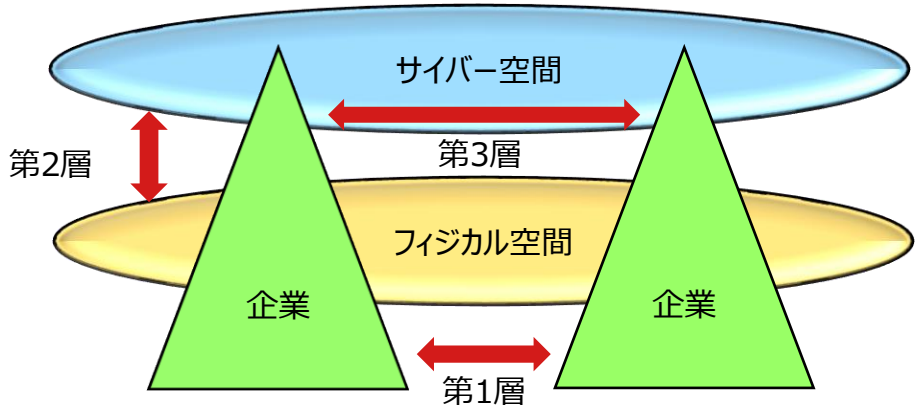
2.2　3層構造モデルと6つの構成要素

CPSにおけるセキュリティ対策フレームワークである、サイバー・フィジカル・セキュリティ対策フレームワーク**(Cyber Physical Security Framework :CPSF)**では、3層構造モデルと6つの構成要素を用いて、各層において検討が必要なセキュリティについて論じている。本書では、本フレームワークを活用し、CPSにおけるトラストについての検討を行う。

➢ 3層構造モデル

サイバーフィジカルシステムを3つの「層」で整理。

第1層：企業間のつながり
第2層：フィジカル空間とサイバー空間のつながり
第3層：サイバー空間におけるつながり



➢ 6つの構成要素

検討対象となる構成要素を6つに整理。
ソシキ、ヒト、モノ、データ、プロシージャ、システム

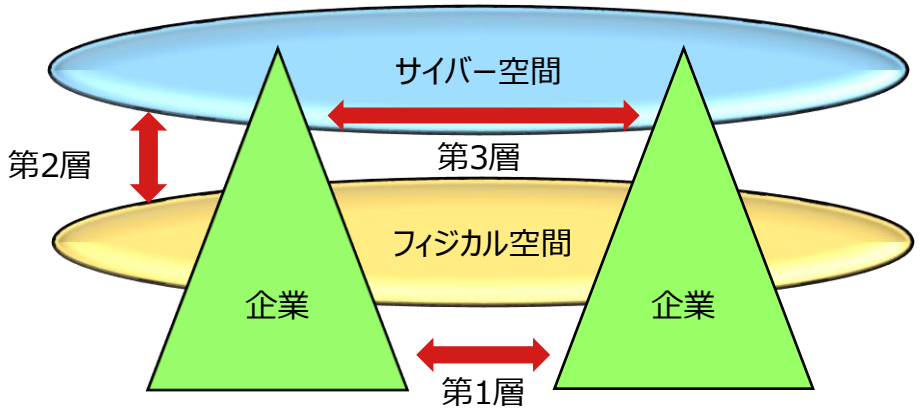
構成要素	定義
ソシキ	バリュークリエイションプロセスに参加する企業・団体・ソシキ
ヒト	組織に属する人、及びバリュークリエイションプロセスに直接参加する人
モノ	ハードウェア、ソフトウェアおよびそれらの部品、操作する機器を含む
データ	フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	定義された目的を達成するために一連の活動を定めたもの
システム	目的を実現するためにモノで構成される仕組み・インフラ

出典：経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要」をもとにDADCが作成

2.3　3層構造モデルを用いたトラストの検討例

トラスト検討の理解を助けるために、国際標準[1],[2]などで定義されたトラストの確立に影響を与えうる特性を活用し、3層構造モデルを用いたトラストの検討例を示す。各層で検討を行う観点については以下の通り整理する。本整理はCPSFを参考に設定しているが、ユースケースによって各層で何を検討すべきか、検討対象が異なる場合があるため、その点はご留意いただきたい。

階層	トラスト検討の観点	検討の概要
第1層	組織・マネジメント	第1層では、フィジカル空間に存在するソシキに注目して検討を行う。フィジカル空間にはソシキ以外にもヒトやモノ、プロシージャなども存在するが、それらはソシキが行うガバナンスやマネジメントによりトラストが担保されるという前提を置く。 例)モノの品質は担保されているのか。 ⇒ ソシキが行う品質管理基準により担保。
第2層	ルールに沿って正しくサイバー空間とフィジカル空間とを転写する機能	第2層では、サイバー空間とフィジカル空間との間の転写において、どのようなルールに従い転写されるのか、またその転写が正しく行われるのか、という点に着目して検討を行う。
第3層	データ	第3層では、サイバー空間上でやり取りされるデータそのものの真正性や、データの発出元が正しいのか等、データに着目して検討を行う。

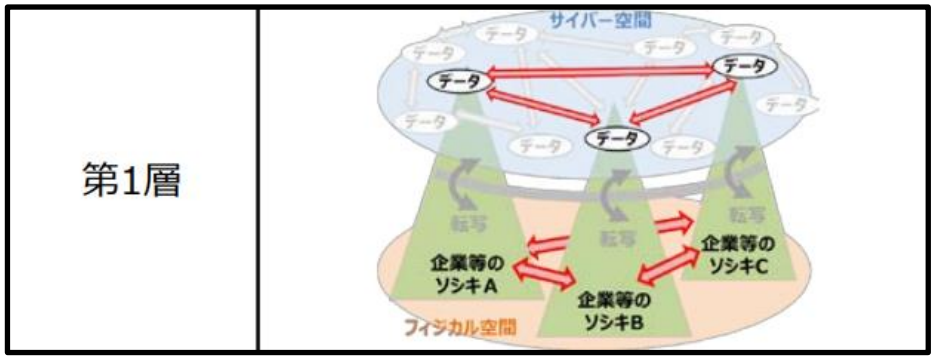


構成要素	定義
ソシキ	バリュークリエイションプロセスに参加する企業・団体・ソシキ
ヒト	組織に属する人、及びバリュークリエイションプロセスに直接参加する人
モノ	ハードウェア、ソフトウェアおよびそれらの部品、操作する機器を含む
データ	フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	定義された目的を達成するために一連の活動を定めたもの
システム	目的を実現するためにモノで構成される仕組み・インフラ

参照：[1]ISO/IEC TS 5723:2022
[2]ISO/IEC 25012:2008(JIS X 25012:2013)

2.4　第1層におけるトラストの検討例

第1層では、企業間のつながりにおける信頼性として、組織・マネジメントに着目して検討を行う。



構成要素	定義
ソシキ	バリュークリエイションプロセスに参加する企業・団体・ソシキ
ヒト	組織に属する人、及びバリュークリエイションプロセスに直接参加する人
モノ	ハードウェア、ソフトウェアおよびそれらの部品、操作する機器を含む
データ	フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	定義された目的を達成するために一連の活動を定めたもの
システム	目的を実現するためにモノで構成される仕組み・インフラ

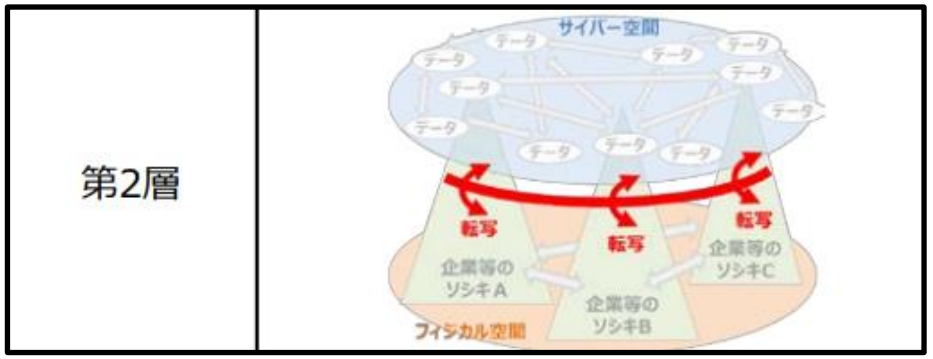
法的要求、商慣習、ビジネス構造などで求められる期待を総合的に判断し、ソシキ間のトラストの確立に資する特性を決定する。そして、決定した特性の検証方法を相手に提供することでトラストワージネスを示し、トラストを確立する。第1層におけるトラストに影響を与える特性とその検証方法を例示する。

特性の例	特性の内容	構成要素	検証すべき項目の例	検証方法の例
真正性(Authenticity) [1]	あるエンティティがその主張通りのものであるか？	ソシキ	Trusteeの主張するソシキは、実際に存在するか？	登記簿、現地調査
標準適合性 (Compliance)	法令、規格、協定又は規範、及び類似の規則を遵守しているか？	ソシキ	ソシキは、業務内容や公告に関わる法令等を遵守しているか？	契約条項、自己評価シート、監査報告書、第三者認証
		ソシキ(ヒト)	ソシキに所属するヒトは、適切に管理されているか？	契約条項、自己評価シート、監査報告書、第三者認証
		ソシキ(モノ)	ソシキの管理下にあるモノは、適切に管理されているか？	契約条項、品質評価基準、監査結果、第三者認証
標準適合性 (データ) (Compliance) [2]	特定の利用状況において、データ品質に関係する、規格、協定又は規範、及び類似の規則を遵守しているか？	ソシキ(データ)	ソシキの管理下にあるデータは、適切に管理されているか？	契約条項、秘密保持契約、自己評価シート、データ仕様書
財務健全性	財務的に健全であるか？	ソシキ	ソシキは、その財務状況は健全であるか？	契約条項、有価証券報告書
答責性 (Accountability) [1]	アクション、決定、パフォーマンスについて説明責任が果たせる(Accountable)状態であるか？	ソシキ	ソシキは、アクション、決定、パフォーマンス、評判などに関わる適切な情報開示を行っているか？	監査報告書、契約書、第三者認定証、人権・環境DD報告書

参照：[1]ISO/IEC TS 5723:2022
[2]ISO/IEC 25012:2008(JIS X 25012:2013)

2.5　第2層におけるトラストの検討例

第2層では、ルールに沿って正しくサイバー空間とフィジカル空間とを転写する機能に着目して検討を行う。



構成要素	定義
ソシキ	バリュークリエイションプロセスに参加する企業・団体・ソシキ
ヒト	組織に属する人、及びバリュークリエイションプロセスに直接参加する人
モノ	ハードウェア、ソフトウェアおよびそれらの部品、操作する機器を含む
データ	フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	定義された目的を達成するために一連の活動を定めたもの
システム	目的を実現するためにモノで構成される仕組み・インフラ

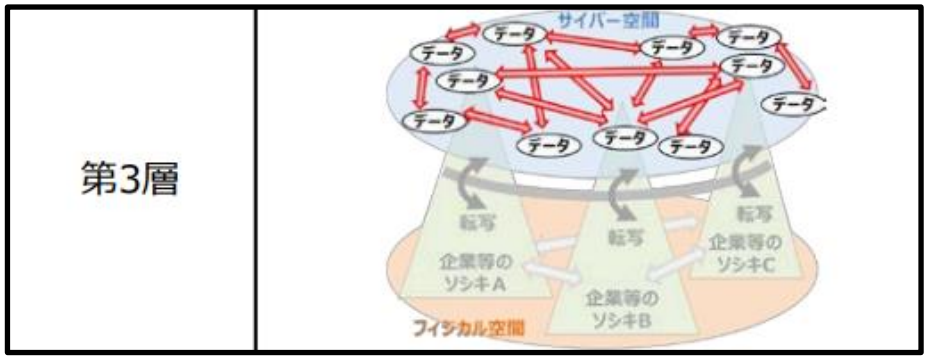
フィジカル空間とサイバー空間の間で転写されるデータが信頼できないものだと、CPS全体としてのトラストは担保できない。特に、第1層で検証した事実を第3層へ転写、またその逆の転写が正しく行われていることを検証することが重要である。各構成要素を転写する機能のトラストの確立に資する特性とその検証方法を例示する。

特性の例	特性の内容	構成要素	検証すべき項目の例	検証方法の例
一貫性(Consistency) [1]	特定の利用状況において、矛盾がないという属性及び他のデータと首尾一貫しているという属性をデータがもつか？	データ、プロシージャ	転写されるデータは、サイバー空間上で一意に特定可能か？	識別子(ID)の一致、データフォーマット、ルール、仕様書、ガイドライン遵守の確認
正確性(Accuracy) [1,2]	観測、計算、推計の結果が、真の値または真と認められた値に近いかどうか？	ソシキ、ヒト	データとして転写するソシキ、ヒトは実在するか？	対面確認、第三者認証
		モノ	データとして転写するモノは実在するか？	実物確認、第三者認証
		データ	データとして転写する数値、項目、数値などは正しいか？	データ仕様書、手順書、タイムスタンプ、第三者認証
真正性(Authenticity) [1]	あるエンティティがその主張通りのものであるか？	ヒト、ソシキ	データの転写を行う対象(ヒト、ソシキ)は、適切な権限を持っているか？	知識認証、生体認証、所有認証
		モノ、システム	データの転写を行う対象(モノ、システム)は、適切な許認可、認証を持っているか。	適合性評価、適合性マーク
完全性　(データ) (Integrity) [1]	データが作成、送信、または保存された時から、不正な方法で変更されていないか？	データ	データは、適切な改ざん防止策が施されているか？	セキュリティ管理策の確認、データに付されたデジタル署名
機密性 (Confidentiality) [2]	特定の利用状況において、承認された利用者によってだけ利用でき、解釈できることが保証されるか？	データ	データは、適切なアクセス制御がなされているか？ データは、適切な方式で暗号化されているか？	セキュリティ管理策の確認、暗号の復号

参照：[1]ISO/IEC TS 5723:2022
[2]ISO/IEC 25012:2008(JIS X 25012:2013)

2.6　第3層におけるトラストの検討例(1/3)

第3層では、サイバー空間上でやり取りされるデータに着目して検討を行う。



構成要素	定義
ソシキ	バリュークリエイションプロセスに参加する企業・団体・ソシキ
ヒト	組織に属する人、及びバリュークリエイションプロセスに直接参加する人
モノ	ハードウェア、ソフトウェアおよびそれらの部品、操作する機器を含む
データ	フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	定義された目的を達成するために一連の活動を定めたもの
システム	目的を実現するためにモノで構成される仕組み・インフラ

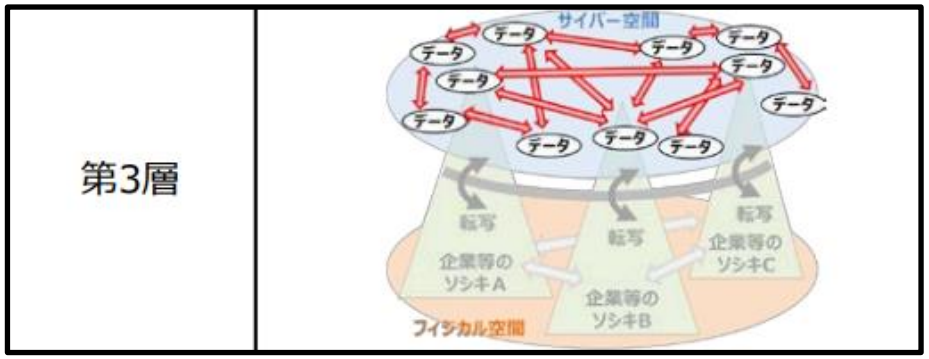
第3層では、データに関わるトラストの確立に資する特性をデータ処理プロセスの観点で抽出した。その特性とその検証方法を例示する。

特性の例	特性の内容	構成要素	検証すべき項目の例	検証方法の例
真正性(Authenticity) [1]	あるエンティティがその主張通りのものであるか？	データ(ヒト)	データの送信元のヒトは、想定しているヒトであるか？	データに付された電子署名
		データ(ソシキ)	データの送信元のソシキは、想定しているソシキであるか？	データに付されたeシール
		データ(システム)	データの送信先のシステムは、想定している接続先であるか？	サーバ証明書
完全性　(データ) (Integrity) [1]	データが作成、送信、または保存された時から、不正な方法で変更されていないか？	データ	データは、適切な改ざん防止策が施されているか？	データに付された電子署名、e-シール、デジタル署名
可用性(Availability) [1]	認可されたエンティティが要求に応じてアクセスでき、使用可能であるという特性	システム	システムは、通信技術的に相互運用が可能か？ システムは、接続ポリシー的に相互運用が可能か？	相互接続試験、トラストポリシー、セキュリティポリシー
セキュリティ(Security) [2]	システムに危害又は損害を与えるように設計された意図的な不正行為に対する耐性を備えているか？	システム	システムに備えられたアプリケーションは、データの送受信や分析・加工などの動作を正しく行っているか？	アプリ認定
正確性(Accuracy) [1,2]	観測、計算、推計の結果が、真の値または真と認められた値に近いかどうか？	データ	データは、送信者と受信者と合意した内容のデータであるか？	データ内容の確認、データ仕様書、第三者認証
標準適合性 (データ) (Compliance) [2]	特定の利用状況において、データ品質に関係する規格、協定又は規範及び類似の規則を遵守しているか？	データ	データは、送信者と受信者と合意した形式のデータであるか？	データ形式、データ仕様書の確認、第三者認証
機密性 (Confidentiality) [2]	特定の利用状況において、承認された利用者によってだけ利用でき、解釈できることが保証されるか？	データ	データは、アクセス制御や暗号化が適切に施されているか？ データの操作履歴は保存されているか？	システム設定、操作ログ

参照：[1]ISO/IEC TS 5723:2022
[2]ISO/IEC 25012:2008(JIS X 25012:2013)

2.6　第3層におけるトラストの検討例(2/3)

第3層では、サイバー空間上でやり取りされるデータに着目して検討を行う。



構成要素	定義
ソシキ	バリュークリエイションプロセスに参加する企業・団体・ソシキ
ヒト	組織に属する人、及びバリュークリエイションプロセスに直接参加する人
モノ	ハードウェア、ソフトウェアおよびそれらの部品、操作する機器を含む
データ	フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	定義された目的を達成するために一連の活動を定めたもの
システム	目的を実現するためにモノで構成される仕組み・インフラ

デジタルデータはアナログデータに比べてなりすましや改ざんが容易であるため、データ受信者は送信者の真正性や受信したデータの完全性、正確性を検証することがトラストの確立につながる。これらの検証を実現するサービスの1つとして、前述した電子署名、eシール、タイムスタンプ等のトラストサービスが挙げられる。

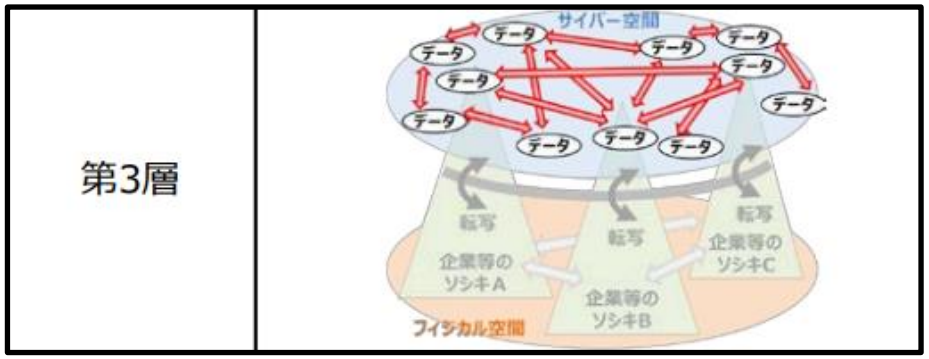
トラストサービスごとに、真正性、完全性、正確性を担保することができるエンティティを整理すると下表のようになる。

トラストサービス	法制度	真正性				完全性	正確性
		ソシキ	ヒト	モノ	システム	データ	データ
電子署名	○	-	○	-	-	○	-
eシール	△(国の指針のみ)	○	-	-	-	○	-
タイムスタンプ	○	-	-	-	-	○	-

電子署名は法制度が存在し、ヒトの真正性やデータの完全性を担保することができる。eシールは国の指針があり、本書執筆時点で法制度化が進められている。eシールはソシキの真正性やデータの完全性を担保することができる。タイムスタンプも法制度が存在し、データの完全性を担保することができる。一方、モノやシステムの真正性、データの正確性については、現状法制度の後ろ盾があるトラストサービスは無い。

2.6　第3層におけるトラストの検討例(3/3)

第3層では、サイバー空間上でやり取りされるデータに着目して検討を行う。

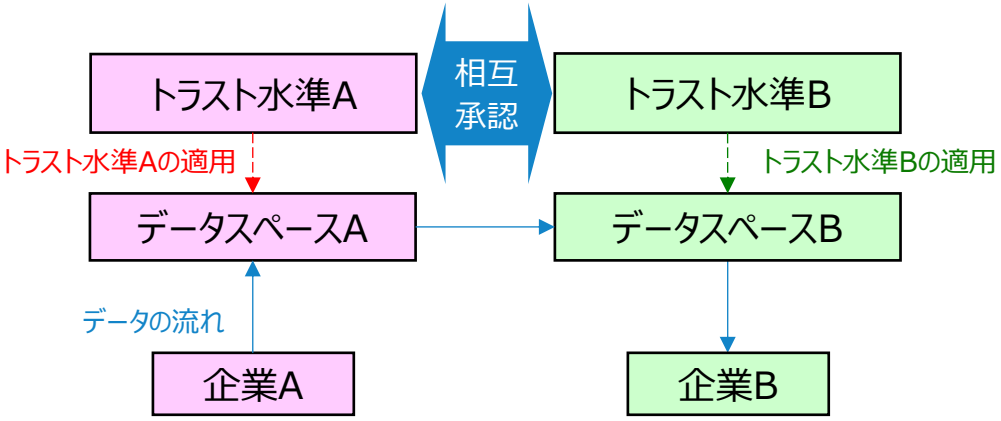


構成要素	定義
ソシキ	バリュークリエイションプロセスに参加する企業・団体・ソシキ
ヒト	組織に属する人、及びバリュークリエイションプロセスに直接参加する人
モノ	ハードウェア、ソフトウェアおよびそれらの部品、操作する機器を含む
データ	フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	定義された目的を達成するために一連の活動を定めたもの
システム	目的を実現するためにモノで構成される仕組み・インフラ

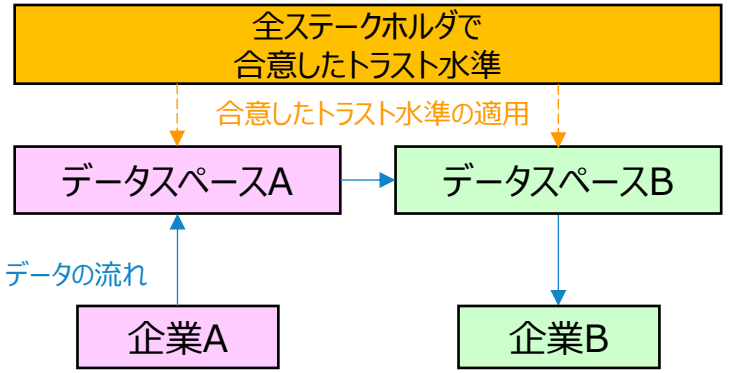
企業や国家をまたいで可用性を確保する(相互運用を可能とする)には、お互いの**トラスト水準**が異なることが課題となる。データ連携の仕組みの1つである**データスペース**(異なる組織・国間(エコシステム)、異業種間でも、信頼性を確保しデータを共有できる標準化された仕組み)を実現するためには、この課題を解決する必要がある。

課題解決の手段として、**①双方のトラスト水準を相互承認**(お互いのトラスト水準を受け入れる)、**②複数のデータスペースで共通のトラスト水準を適用**、**③共通のデータスペースを利用しトラスト水準を統一**、などが挙げられる。

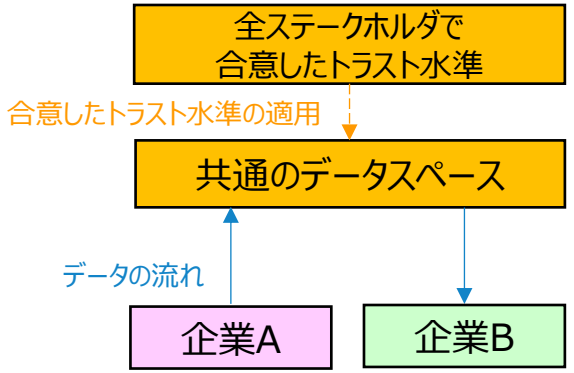
①双方のトラスト水準を相互承認



②複数のデータスペースで共通のトラスト水準を適用



③共通のデータスペースを利用しトラスト水準を統一



Digital Architecture Design Center　出典：情報処理推進機構 デジタル基盤センター データスペース入門

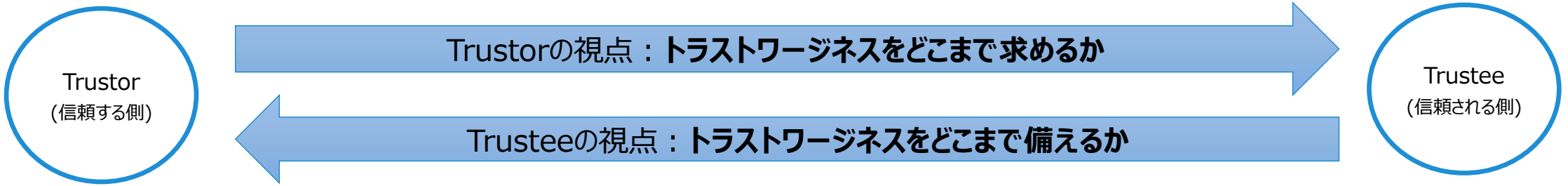
2.7　検証しない場合のリスクとトラストワージネス

ここまで、各層における検証に資する特性の例を記載してきたが、各特性を検証しない場合に想定されるリスクについて、いくつか例示する。

階層	特性の例	検証しない場合に想定されるリスクの例
第1層	**標準適合性(Compliance)** 法令、規格、協定又は規範、及び類似の規則を遵守しているか？	・社員のコンプライアンス違反による会社の信頼低下 ・営業秘密の漏えいによる事業影響
第2層	**正確性(Accuracy)** 観測、計算、推計の結果が、真の値または真と認められた値に近いかどうか？ **完全性(Integrity)** データが作成、送信、または保存された時から、不正な方法で変更されていないか？	・内部に不正アクセスされたシステムが意図しない動作 ・改ざんされたソフトウェアによる正確でないデータの送信等が発生
第3層	**真正性(Authenticity)** あるエンティティがその主張通りのものであるか？ **機密性(Confidentiality)** 特定の利用状況において、承認された利用者によってだけ利用でき、解釈できることが保証されるか？	・サイバー空間にて取り扱われる保護すべきデータの漏えい ・なりすましされたシステム等から不適切なデータを受領

このように、十分な検証をせずに容易にトラストを確立してしまうと、期待を裏切られる可能性が高くなる。もちろん、例示した特性をすべて検証しても、期待が裏切られる可能性をゼロにできるわけではない。Trustorによる検証が難しい特性も存在するだろう。しかし、検証を行うことによって、期待が裏切られる可能性を低減させることができる。どこまでその可能性を低減できればトラストが確立できるのかは、Trustorの主観的な判断による。

リスクやコスト、時間的制約などを総合的に判断し、トラストを確立できる期待値を設定し、Trusteeに要求するトラストワージネスを示していくことが今後のデジタル社会においてTrustorにとって必要なことになるだろう。一方、Trustorの期待に応えるトラストワージネスを準備をしておくことが、Trusteeにとって求められることだろう。



2.8　各層における検証方法

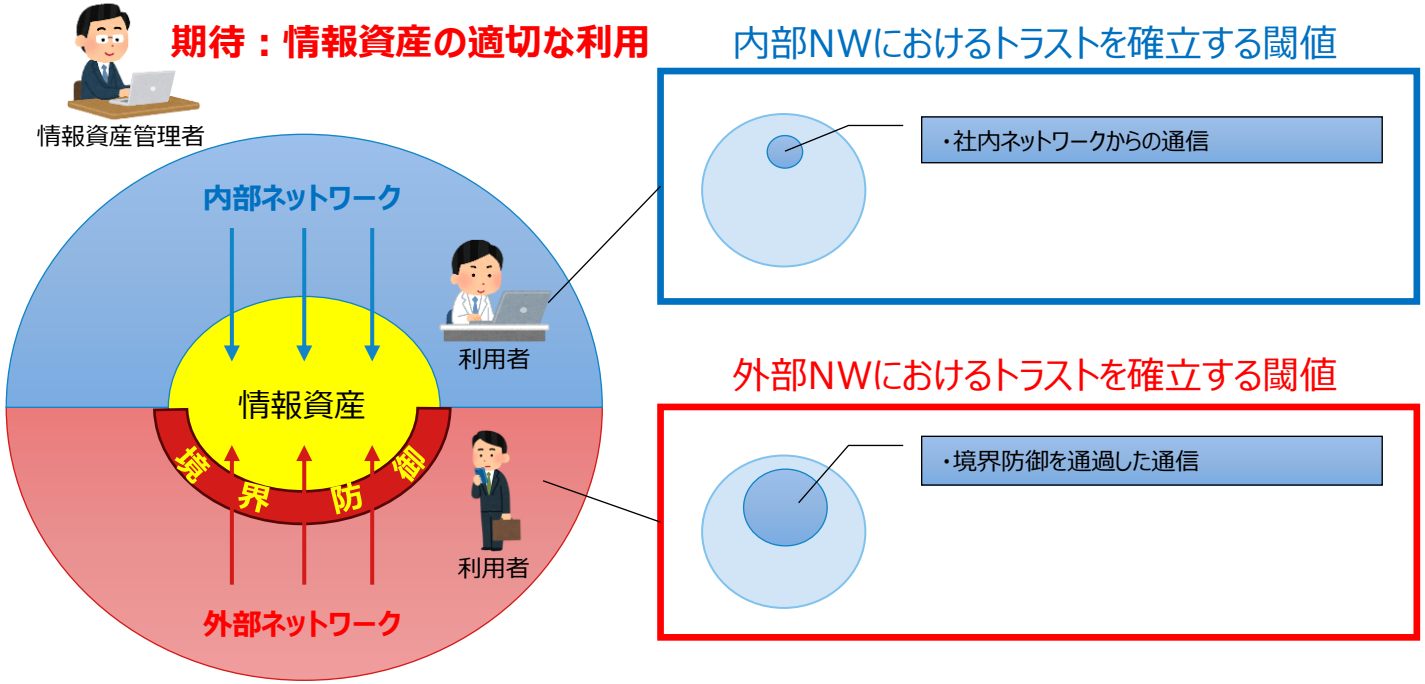
本章では、CPSFのアプローチを参考に、各層におけるトラストの確立に資する特性について例示してきたが、あくまでも理解を助けるための例示であり、検討の規範や検証すべき特性の必要十分性を示すものではない。挙げた特性が全てではないし、また挙げた特性をすべて検証できればトラストを確立してよいということでもない。重要なのは、どこまで検証できればトラストを確立できるのか、である。トラスト検討のアプローチ例として役立ててほしい。最後に各層で示した検証方法の例を示す。

特性	第1層		第2層		第3層	
	検証方法の例	構成要素	検証方法の例	構成要素	検証方法の例	構成要素
真正性 (Authenticity) [1]	登記簿、現地調査	ソシキ	知識認証、生体認証、所有認証	ソシキ、ヒト	-	-
	-	-	適合性評価、適合性マーク	モノ、システム	-	-
	-	-	-	-	データに付された電子署名・e-シール、サーバー証明書	データ
標準適合性 (Compliance)	契約条項、自己評価シート、監査報告書、第三者認証	ソシキ	-	-	-	-
	契約条項、自己評価シート、監査報告書、第三者認証	ソシキ(ヒト)	-	-	-	
	契約条項、品質評価基準、監査結果、第三者認証	ソシキ(モノ)	-	-	-	
標準適合性 (データ) (Compliance) [2]	契約条項、秘密保持契約、自己評価シート、データ仕様書	ソシキ(データ)	-	-	データ形式、データ仕様書の確認結果、第三者認証	データ
	-	-	-	-	-	-
	-	-	-	-	-	-
財務健全性	契約条項、有価証券報告書	ソシキ	-	-	-	-
答責性 (Accountability) [1]	監査報告書、契約書、第三者認定証、人権・環境DD報告書	ソシキ	-	-	-	-
一貫性 (Consistency) [1]	-	-	識別子(ID)の一致、データフォーマット、ルール、仕様書、ガイドライン遵守の確認	データ、プロシージャ	-	-
正確性 (Accuracy) [1,2]	-	-	対面確認、第三者認証	ソシキ、ヒト	-	-
	-	-	実物確認、第三者認証	モノ	-	-
	-	-	データ仕様書、手順書、タイムスタンプ、第三者認証	データ	データ内容の確認結果、データ仕様書、第三者認証	データ
完全性　(データ) (Integrity) [1]	-	-	セキュリティ管理策の確認結果、データに付されたデジタル署名	データ	データに付された電子署名、e-シール、デジタル署名	データ
機密性 (Confidentiality) [2]	-	-	セキュリティ管理策の確認、暗号の復号	データ	システム設定、操作ログ	データ
可用性 (Availability) [1]	-	-	-	-	相互接続試験の結果、トラストポリシー、セキュリティポリシー	システム
セキュリティ (Security)[2]	-	-	識別子(ID)、データフォーマット	プロシージャ	アプリ認定	システム

参照：[1]ISO/IEC TS 5723:2022
[2]ISO/IEC 25012:2008(JIS X 25012:2013)

補足　ゼロトラストセキュリティ

トラストが関わるものとして、ゼロトラストと呼ばれるセキュリティモデルが存在する。本スライドでは、ゼロトラストの概念を解説する。
従来、内部ネットワークは信頼し、外部ネットワークは信頼しないとする管理が一般的であった。具体例として、内部ネットワークに接続する従業員などは信頼できると考え、アクセス制御や認証・認可を省略して情報資産へのアクセスを許可するが、外部ネットワークには信頼できない不正者が存在すると考え、外部からのアクセスに対しては、境界型セキュリティ(例えばユーザ認証システムやFW(Firewall)、WAF(Web Application Firewall)などを利用して実現。)を施す管理方法が挙げられる。すなわち、内部ネットワークの利用者には暗黙的なトラスト(Implicit Trust)が確立しているが、外部ネットワークからの利用者にはある種の明示的なトラスト(Explicit Trust)の確立を求めるものとなっている。

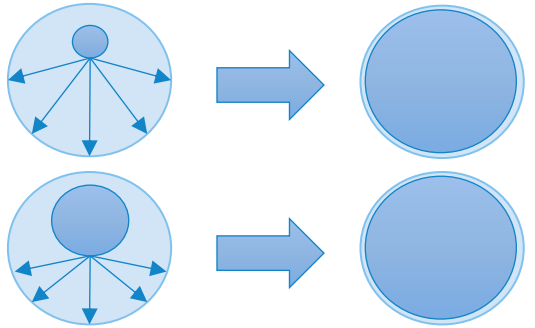


社内ネットワークからの通信であれば、
「情報資産の適切な利用」がなされると信じ、トラストを確立する。

直接確認(検証)していないが、大丈夫だとみなす領域

境界防御を通過してきた通信であれば、
「情報資産の適切な利用」がなされると信じ、トラストを確立する。

ゼロトラストの基本的な概念は、「誰も暗黙的に信頼しない、常に検証する」という考え方である。つまり、内部ネットワークも外部ネットワークと同様に扱い、すべてのアクセスを疑い、検証することを前提とし、認証・認可の強化や権限の最小化といった様々なセキュリティ対策で実現される。ゼロトラストは右図のように、暗黙的なトラストに頼る部分を削減し、トラストワージネスにより明示的なトラストに置き換えるという考え方とも解釈できる。



ゼロトラストネットワークは、内部通信、外部通信いずれも同等に信頼せず、検証可能な範囲を広げ、根拠なく信頼する範囲を限りなくゼロに近づけることにより、リスクを低減するという考え方。

Appendix：用語集

本書における用語定義を以下に示す。

Term	用語	定義
Conformity Assessment Body	適合性評価機関	製品、サービス、システムなどを対象に、特定の要件への適合性を評価する独立した機関。公平性と信頼性を保つために、通常は第三者機関として運営される。
Cyber Physical Security Framework(CPSF)	-	バリュークリエイションプロセスのリスク源を適切に捉えるためのモデルを構築し、求められるセキュリティ対策の全体像を整理するとともに、産業界が自らの対策に活用できるセキュリティ対策例をまとめたもの。
Cyber Physical System(CPS)	-	Society5.0において実現していくべきサイバー空間とフィジカル空間を高度に融合させたシステム。
Data Space	データスペース	異なる組織・国間(エコシステム)、異業種間でも、信頼性を確保しデータを共有できる標準化された仕組み。
Digital Signature	デジタル署名	電子データの作成者を示す目的で行われる公開鍵暗号技術に基づく措置であり、デジタル署名が付されて以降、当該電子データが改変されていないことを確認可能とする仕組み。
Digital Trust	デジタルトラスト	デジタル空間において、人・組織・モノ・データ・プロシージャ・システムが、ステークホルダーからの信頼を得られている状態。
Electronic Delivery	eデリバリー	電子データの送信・受信の証明や送受信されるデータの完全性の確保を実現する仕組み。
Electronic Seal	eシール	電子データの発行元の組織等を示す目的で付与されるデータであり、付与されて以降、当該電子データが改変されていないことを確認可能とする仕組み。
Electronic Signature	電子署名	手書きの署名や押印と同等の法的効力を持つ電子データやデジタル署名。
Explicit Trust	明示的なトラスト	検証できない特性を元に確立したトラスト。
Implicit Trust	暗黙的なトラスト	特性を検証した上で確立したトラスト。
Public Key Infrastructure(PKI)	公開鍵基盤	公開鍵暗号方式に基づく電子認証の技術基盤。
Society5.0	-	サイバー空間とフィジカル空間を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する人間中心の社会。
Stakeholder	ステークホルダ	企業活動において直接・間接的に影響を受ける利害関係者。
Timestamp	タイムスタンプ	電子データがある時刻に存在し、その時刻以降に当該電子データが改変されていないことを証明する仕組み。
Trust	トラスト	相手が期待を裏切らないと思える状態。
Trust Anchor	トラストアンカー	信頼の基点となる証明書等の発行業務を担っている組織、またはその組織にその業務を行うことを認めた(認定した)組織。
Trust Service	トラストサービス	データの正当性や改ざん防止を保証するための電子的な仕組み。
Trust Service Provider	トラストサービスプロバイダ	複数のトラストサービスを提供する自然人もしくは法人(EU規則No910/2014 eIDAS)。
Trustee	-	信頼される側。
Trustor	-	信頼する側。
Trustworthiness	トラストワージネス	相手の期待に対して検証可能な方法で応える能力。
-	特性	TrusteeとTrustorのトラストに影響を与える性質や特徴。
-	対象真正性	人であれば相手が本人なのか、物であれば本物なのかを示す特性。
-	内容真実性	示された内容が本当に正しいのかを示す特性。
-	振る舞い予想・対応可能性	相手が期待通りに振る舞ってくれるかどうか、また期待通り振る舞ってくれなった場合、そのリカバリや補償の対応を行う能力を有しているかを示す特性。

Appendix :
ISO/IEC TS 5723:2022 Trustworthiness — Vocabulary

システムおよびその関連サービスの信頼性に関する用語を定義した規格。トラストワージネス(Trustworthiness)は「利害関係者の期待に対して検証可能な方法で応える能力」と定義して、トラストワージネスに関わる15の特性を例示している。

用語	定義
説明責任、答責性(Accountability)	アクション、決定、パフォーマンスについて説明責任が果たせる(Accountable)状態。
正確性(Accuracy)	観測、計算、推計の結果が、真の値または真と認められた値に近いかどうかの尺度。
真正性(Authenticity)	あるエンティティがその主張通りのものであるという特性。
可用性(Availability)	認可されたエンティティが要求に応じてアクセスでき、使用可能であるという特性。
制御性(Controllability)	人間または他の外部エージェントがシステムの機能に介入できるシステムの特性。
完全性(Integrity)	-
完全性(データ)	データが作成、送信、または保存された時から、不正な方法で変更されていないという特性。
完全性(システム)	正確性(Accuracy)と完全性(Completeness)。
プライバシー(Privacy)	個人の私生活や事柄に立ち入らない自由。
品質(Quality)	-
品質(データ)	指定された条件下で使用されたときに、データの特性が明示的・暗黙的なニーズを満たす度合い。
品質(システム)	オブジェクトに固有の特性の集合が、要求事項を満たす度合い。
信頼性(Reliability)	-
信頼性(セキュリティ)	意図した動作や結果が一貫しているという特性。
信頼性(システム)	与えられた条件下で、与えられた時間間隔の間、故障することなく要求されたとおりに機能するアイテムの能力。
回復力(Resilience)	-
回復力(ガバナンス)	自然のものであれ人為的なものであれ、潜在的に破壊的な事象を予測し、それに適応し、それに対抗し、あるいはそこから迅速に回復する能力。
回復力(システム)	内外の変化に直面してもその機能と構造を維持し、必要な場合には潔く劣化するシステムの能力。
堅牢性(Robustness)	システムが様々な状況下でその性能レベルを維持する能力。
安全性(Safety)	定義された条件下で、人の生命、健康、財産又は環境が危険にさらされる状態に至らないようなシステムの特性。
セキュリティ(Security)	システムに危害又は損害を与えるように設計された意図的な不正行為に対する耐性。
透明性(Transparency)	-
透明性(情報)	開かれた、包括的な、アクセス可能な、明快で理解可能な情報の提示。
透明性(システム)	公開性と説明責任を意味するシステムまたはプロセスの特性。
ユーザビリティ(Usability)	システム製品またはサービスを特定の利用者が使用し、特定の使用状況において、有効性、効率性及び満足度をもって特定の目標を達成できる度合。

Appendix :
ISO/IEC 25012:2008 (JIS X 25012:2013) : ソフトウェア製品の品質要求及び評価（SQuaRE）–データ品質モデル

ソフトウェア工学におけるデータ品質モデルを定義した規格。ソフトウェアの処理に影響を与える15のデータ特性を定義している。

用語	定義
正確性(Accuracy)	特定の利用状況において、意図した概念又は事象の属性の真の値を正しく表現する属性をデータがもつ度合い。
完全性(Completeness)	実体に関連する対象データが、特定の利用状況において、全ての期待された属性及び関係する実体インスタンスに対する値をもつ度合い。
一貫性(Consistency)	特定の利用状況において、矛盾がないという属性及び他のデータと首尾一貫しているという属性をデータがもつ度合い。それは、一つの実体に関するデータ相互間、又は同等の実体に対する類似のデータをまたがったデータ同士間の、いずれか一方又は両方となる場合がある。
信ぴょう性(Credibility)	特定の利用状況において、利用者によって真(実)で信頼できるとみなされる属性をデータがもつ度合い。注記 信ぴょう(憑)性は、真正性(authenticity)(素性、帰属、約束の正しさ)の概念を含む。
最新性(Currentness)	特定の利用状況において、データが最新の値である属性をもつ度合い。
アクセシビリティ(Accessibility)	特に、幾つかの障害が原因で、支援技術又は特別の機器構成を必要とする人々が、特定の利用状況において、データにアクセスできる度合い。
標準適合性(Compliance)	特定の利用状況において、データ品質に関係する、規格、協定又は規範、及び類似の規則を遵守する属性をデータがもつ度合い。
機密性(Confidentiality)	特定の利用状況において、承認された利用者によってだけ利用でき、解釈できることを保証する属性をデータがもつ度合い。
効率性(Efficiency)	特定の利用状況において、適切な量及び種類の資源を使用することによって処理することができ、期待された水準の性能を提供できる属性をデータがもつ度合い。
精度(Precision)	正確な属性、又は特定の利用状況において弁別を提供する属性をデータがもつ度合い。
追跡可能性	特定の利用状況において、データへのアクセス及びデータに実施された変更の監査証跡を提供する属性をデータがもつ度合い。
理解性(Understandability)	利用者がデータを読み、説明することができる属性で、特定の利用状況において、適切な言語、シンボル及び単位で表現された属性をデータがもつ度合い。
可用性(Availability)	特定の利用状況において、承認された利用者及び／又はアプリケーションがデータを検索できる属性をデータがもつ度合い。
移植性(Portability)	特定の利用状況において、既存の品質を維持しながら、データを一つのシステムから他のシステムに実装したり、置き換えたり、移動したりできる属性をデータがもつ度合い。
回復性(Recoverability)	特定の利用状況において、故障発生の場合でさえ、明示された水準の操作及び品質を継続し、維持することを可能にする属性をデータがもつ度合い。

おわりに

本書では、トラストの概念とその重要性、特にデジタル社会におけるトラスト確立の必要性について解説した。デジタル化や技術の進展が進む中で、我々の生活やビジネス環境は急速に変化している。このような状況において、「トラスト」は単なる言葉の概念を超え、情報やデータの流通、取引の安全性を確保するための情報基盤の一部を形成する、必要不可欠な存在にもなってきている。

相手が実在する本人なのか(対象真正性)、相手の言っていることは正しいのか(内容真実性)、約束は守ってくれるのか(振る舞い予想)、守らなかった場合の補償、もしくはリカバリ策はあるのか(対応可能性)、そしてそれらを示す特性をどの層で、どのように検証していくのか。そしてステークホルダの合意を得るために、コストと効果のバランスを見て実現可能な方法を考えていくこと、それがSociety5.0におけるトラスト検討の重要な要素となりえるだろう。

最後に、本書がトラストに関する理解を深め、今後の議論や実践に役立つ一助となることを願い、結びの文とさせていただく。

著作・執筆および協力者のご紹介（敬称略、50音順、所属は公開時のもの）

【著作・製作】	独立行政法人情報処理推進機構(IPA) デジタルアーキテクチャ・デザインセンター	
【執筆】	デジタルアーキテクチャ・デザインセンター	井上　達紀
		川端　健
		中村　洋介
		花谷　嘉一
		武藏　大祐
【専門委員】	株式会社Maximax	濱口　総志
	株式会社エヴァアビエーション	亀田　繁
		久野　保之
		高塚　肇
【協力】	経済産業省　商務情報政策局　情報経済課※	磯部　光平

※所属組織としての公式見解を示すものではない。

お問い合せ先

本件に関するお問い合わせは、以下の連絡先へお寄せください。

IPA デジタルアーキテクチャ・デザインセンター
E-mail：dadc-info★ipa.go.jp

［★］を［@］に置き換えてください。