激化するサイバー脅威と、信頼性と自由なデータ流通を支えるデジタルトラスト

2023/11/8

デジタルトラスト協議会
NECサイバーセキュリティ戦略統括部　Executive Professional
林　亮平, CISSP(Certified Information Systems Security Professional)

JDTF
JAPAN DIGITAL TRUST FORUM

本日お伝えしたいこと

- **デジタル化・サイバー空間を利用した経済活動によって**今までの制約(物理、距離、時間)が縮小し、**経済合理性が良くなった**(**いわゆるDX化の進展**)。
- **その一方、**データはサイバー空間で論理的に存在・流通し何かしら処理・利用されるため、サイバー空間の経済活動を狙った脅威が増大。**年々脅威が顕在化し大きなインパクトを与える**(会社(国家?)の存続に関わるような)**インシデントが多発。**
- 経済活動は**デジタル依存度が高まり、悪用する輩が増え**た。つまり**信頼出来ないデータ(改変された、消された、etc)を利用することで経営リスクが増大。**
- **トラストを確保することは経営における説明責任を果たすためにも重要**
  (行為や決定から生じた結果に対して、状況の説明、原因の究明など、事後の対応を行わなければならない義務または責任)
- **Digital Trustに関わる法令、ガイドライン、ガイダンス、レギュレーションが出てきている。**グローバル化の経済では単一的な対応では無く**国際通用性を踏まえた対応**が必要。

→Digital Trustは幅も広く、奥行きも深いので、是非JDTFにご相談ください。

→競争力を維持、向上させるためにもDXは避けられない。
＝　信頼性と自由なデータ流通の普及には産業界で協力することがとても大切。

アジェンダ

1．自己紹介とJDTFの紹介
2．激化するサイバー脅威
3．セキュリティとトラストの関係
4．日本や欧州等におけるデータ流通、トラストに関する動向
5．具体的な社会課題と手段としてのトラストサービス
6．まとめ

１．自己紹介と
デジタルトラスト協議会の紹介

自己紹介

林 亮平　（Ryohei Hayashi）

CISSP（Certified Information Systems Security Professional）

一般社団法人デジタルトラスト協議会　運営会議構成員
NEC サイバーセキュリティ戦略統括部 Executive Professional
兼　セキュリティ事業統括部、兼　CISO統括オフィス

- NEC入社以来、メインフレーム及びオープンシステムの製品計画、パートナアライアンス・M&A戦略推進、ミッションクリティカルシステム事業、パブリックセーフティ事業、サイバーセキュリティ事業等を担当。
- 2017年、東京2020組織委に出向。テクノロジーサービス局次長として、大会を支えるハイブリッドクラウド、マルチベンダシステムPJを推進し、大会本番時は、24×７のテクノロジーオペレーションを統括。
- 2022年よりデジタルトラスト協議会に参画し、トラストサービスの政策提言、普及活動に取り組む。

(一社)デジタルトラスト協議会　ご紹介

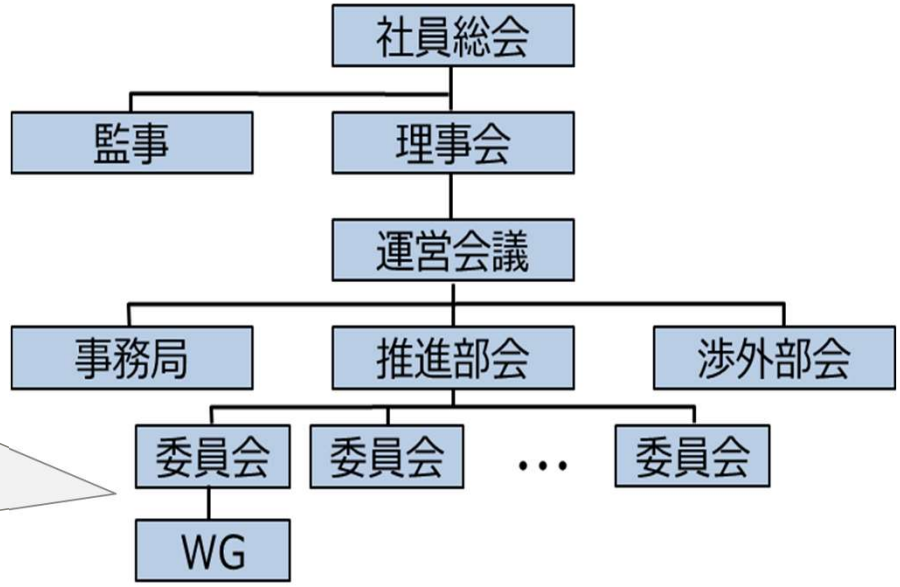
- 団体名：一般社団法人デジタルトラスト協議会（JDTF(*)）（2022/2/4設立）
- 目的：デジタル社会における新たなイノベーション創出の基礎となるデジタルトラストの実現
- 会員数：正会員３３団体 、賛助会員５団体、特別会員１８団体･個人（2023/5/1現在）

(*) JDTF : Japan Digital Trust Forum
URL: https://jdtf.or.jp/

我が国のデジタルトラスト基盤の創設･発展及び国際協調の学界･民間の受け皿としての位置づけの強化を目的として新団体を設立

- ルール形成委員会
- ビジネスプロセス withﾄﾗｽﾄ委員会
- Trusted Digital ID委員会
- サプライチェーン改革委員会
- 調査研究委員会
- 普及促進委員会
- トラストサービスの在り方検討委員会
- デジタルトラスト制度検討委員会
- DADCタスクフォース
- AATL認証タスクフォース
- TaaS(Trust as a Service)タスクフォース

JDTF(*)組織体制

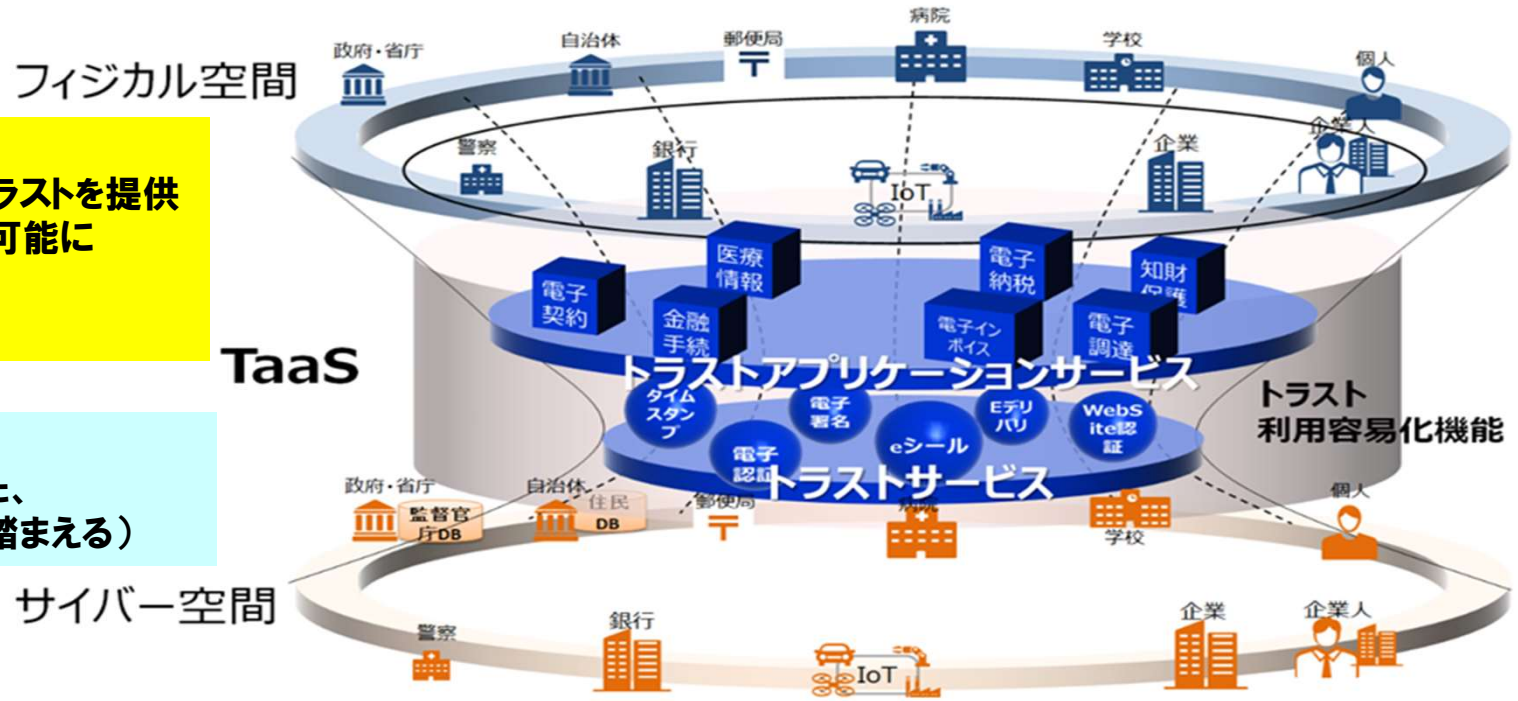


(一社)デジタルトラスト協議会　ご紹介

相手やデータの正しさが見えないゼロトラスト環境下で、人や組織間のデジタル化された手続きを堅牢かつ確実に実現する（堅確化）ために必要となる仕組み・制度を提言
繋がる相手／データの保証をより容易に利用できるようにするTaaS(Trust as a Service)の推進

実現の仕組み：
・様々な組織・個人に対し、サービス型のトラストを提供
・それぞれのトラストサービス間での協調が可能に
・1ストップでの情報集約が可能
・サイバー空間内での高速な処理を実現

ルール・制度：
・フィジカル空間の手続きの厳格さに応じた、運用や仕組みに関する水準（国際連携を踏まえる）

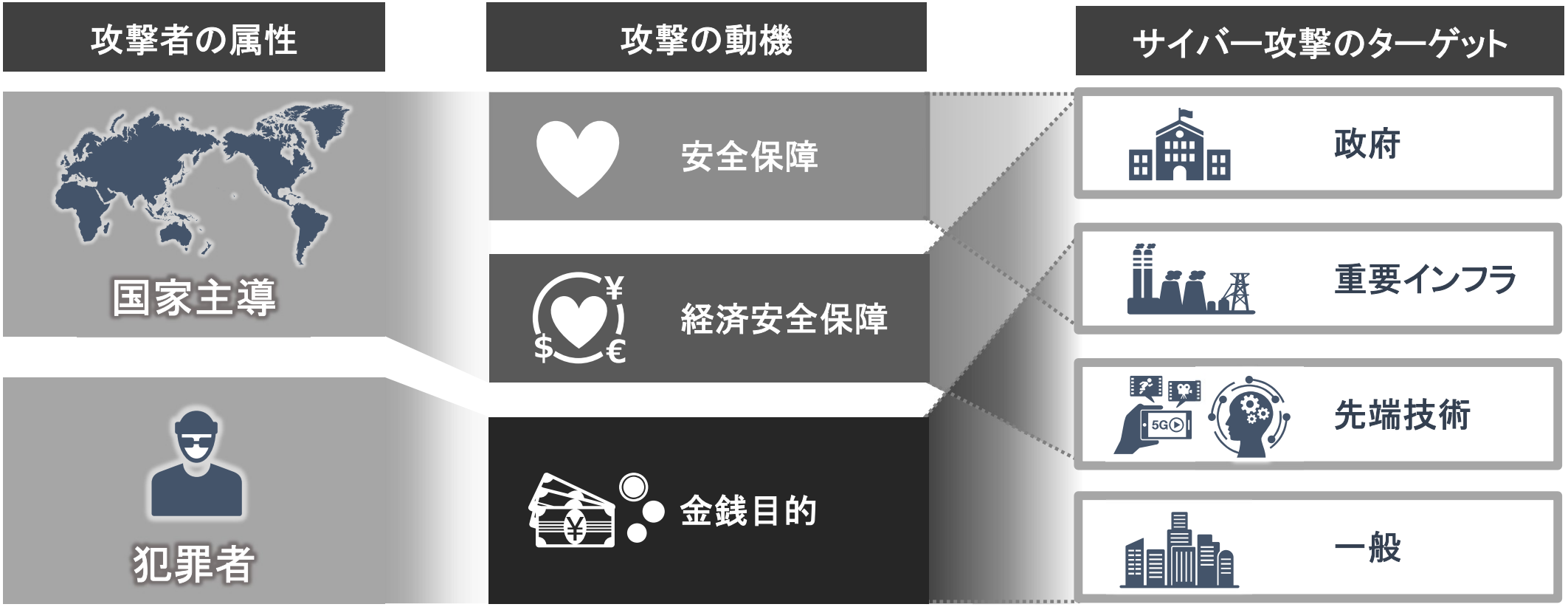


JDTFが実現をめざす新たな仕組み　-TaaS-

２．激化するサイバー脅威

セキュリティリスクの変化 ＜攻撃ターゲット＞

- 地政学的な状況の変化に伴い、民間企業も 国家的な攻撃の標的に
- 特に先端技術を保有する企業は、経済安全保障を動機としたリスクが増大



出典：NEC

サイバーセキュリティリスクの動向 ＜経営インパクト＞

- DXが急速に進む一方で、経済目的でのサイバー攻撃が激化
- あらゆるシステム・データが標的となり、企業の事業継続が脅かされている

ランサムウェア被害※

被害報告件数 約5倍
令和2年下半期21件→令和4年下半期116件
（警察庁に報告があった件数）

被害対象：企業規模を問わず広範に
大企業27% 中小企業53%

感染経路
VPN機器、リモートデスクトップからの侵入 81%

脆弱性公表直後から
脆弱性を標的
としたアクセス急増

サイバー攻撃による経営インパクト（例）

基幹システム停止
決算発表を延期

製造業大手

国内十数工場
稼働停止

大手部品メーカー

サイバー攻撃の調査／
復旧費用
特別損失 **数億円**

コンサル大手

DX化によりシステム間連携が進むことで、被害は1つの企業に閉じない

※ 出典：令和4年におけるサイバー空間をめぐる脅威の情勢等について（警察庁 令和5年3月16日）https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

出典：NEC

国内外のインシデント事例

○ サイバー攻撃による情報の漏えいやシステムの停止等が企業・組織・個人の活動に重大な影響を与える事案が国内外で発生。

１．国内の事例

2021年 5月 富士通のプロジェクト情報共有ツール「ProjectWEB」への不正アクセスにより、同ツールを利用していた内閣官房NISC、国交省、外務省等から利用する情報システム等の情報が流出したとの発表。

7月 国内大手製粉会社ニップンが大規模なサイバー攻撃を受け約9割のシステムに被害、決算報告にも影響。

9月 Fortinet製VPN機器から認証情報が流出、中小企業を中心に日本企業約1000社が含まれるとの報道。

10月 NTTドコモが同社を騙ったSMSによるフィッシング詐欺で、およそ1200人、１億円の被害が発生したと発表。

10月 オリパラ組織委員会が大会期間中に4.5億回のサイバー攻撃を観測、全てブロックし影響無しと発表。

11月 徳島県の町立病院がランサムウェアによる攻撃を受け、電子カルテが暗号化。予約の受け入れなどを停止。

2022年 2月 メールの添付ファイル開封によるEmotetの感染が再拡大、国内の複数企業が感染を公表。

2月 自動車部品メーカへのサイバー攻撃により、トヨタ自動車が国内全工場の稼働を１日停止。

9月 e-Gov等の政府サイト等にDDoS攻撃による閲覧障害が発生。ハッカー集団「キルネット」が犯行声明。

10月 大阪府の総合病院がランサムウェアによる攻撃を受け、電子カルテが暗号化。外来診療や通常の手術などを停止。

2023年 7月 名古屋港がランサムウェアによる攻撃を受け、2日以上にわたりコンテナ搬入等が停止。ハッカー集団「ロックビット」が犯行声明。

２．外国の事例

2020年12月 米国のソフトウェア企業であるSolarWinds（ソーラーウィンズ）社がハッキングされ、同社が提供するネットワーク管理ソフトウェア製品を導入している企業や政府機関の内部情報などが流出したことが判明。

2021年 5月 ベルギーのISPであるBelnetがDDoS攻撃を受け、政府機関ウェブサイトなどがダウンしたとの報道。

5月 米国の石油パイプライン大手のColonial Pipeline（コロニアルパイプライン）社が、ランサムウェアによるサイバー攻撃を受けて操業を一時停止し、原油価格にも影響。

7月 米国のIT企業Kaseyaのリモート監視・管理製品がゼロデイ攻撃を受け、同製品を運用するMSP（Managed Service Provider）を通して、MSPサービスを利用する多数の中小企業等でランサムウェアによる被害が発生。

8月～9月 米・露・ニュージーランドなど世界各地でボットネット「Meris」によるものとみられるDDoS攻撃が発生。

10月 米国テレビ局運営大手Sinclairがランサムウェア攻撃を受け、傘下の複数のテレビ局で放送が停止。

2022年 2月 ウクライナの政府機関、大手金融機関などに対するサイバー攻撃が発生

出典：総務省におけるトラストサービスの取組について

元CIAのCISOが提言したセキュリティ対策とゼロトラスト

JDTF JAPAN DIGITAL TRUST FORUM

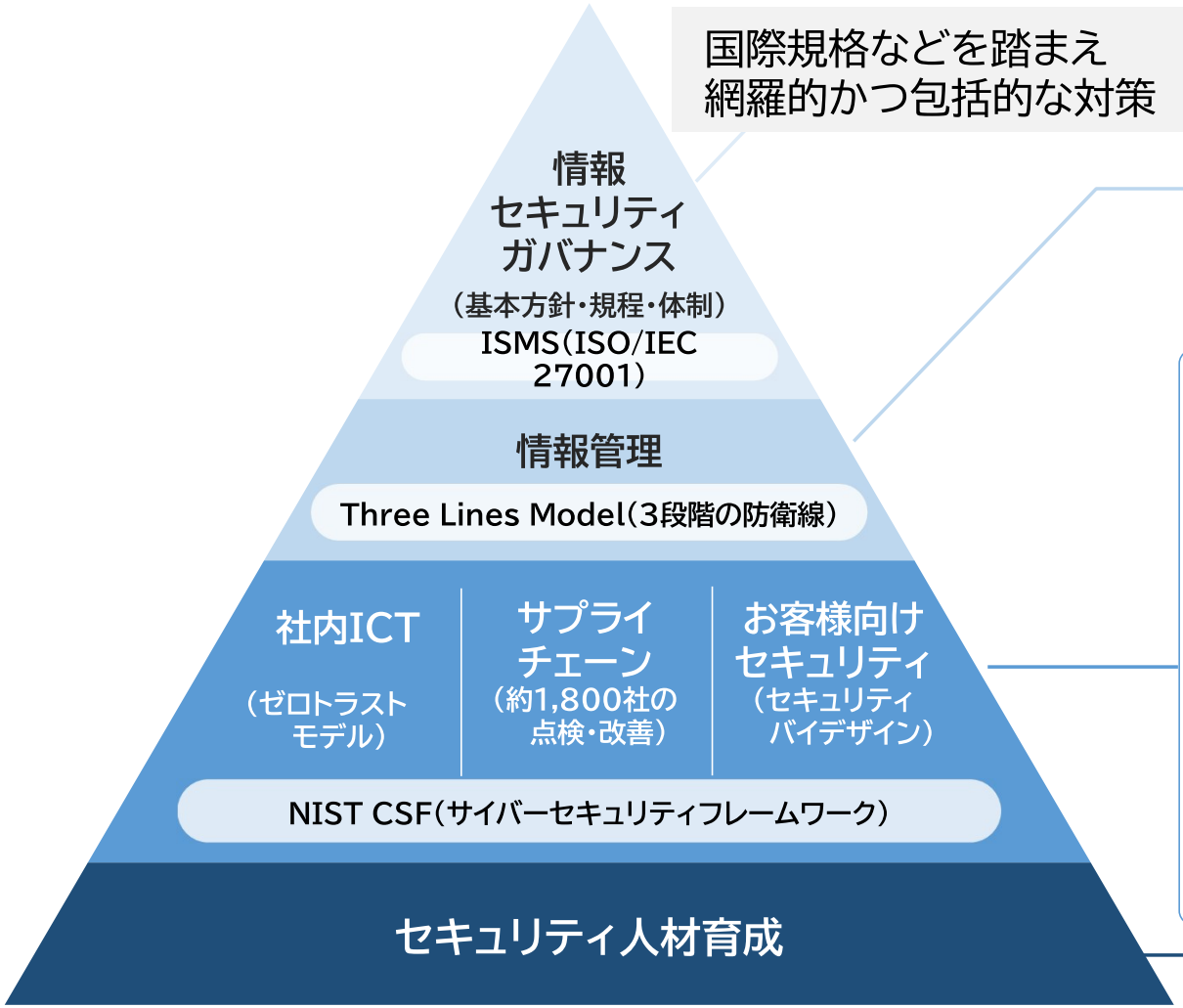
認証を取られてインシデントに繋がるパターンが大半！

- ビッグマン氏が挙げた６つの基本的な「原則」

1. セキュリティが強化されたイメージ（ソフトウェア）を利用
2. **二要素認証やスマートカードを組み合わせる等して認証を強化**
3. **ルート権限、管理者権限を持つアカウントのクレデンシャル管理を徹底**
4. ネットワークレベルでのセグメンテーション（分離）
5. エンドポイントにおいてカーネルやメモリを保護
6. 脆弱性管理

出典：@ITセキュリティセミナ「一にも二にも「防御」を――元CIAのCISOが提言した6つのセキュリティ対策」を元に作成
https://atmarkit.itmedia.co.jp/ait/articles/1903/12/news014.html

例:NECグループのセキュリティ全体像



情報セキュリティガバナンス(基本方針・規程・体制)
- サイバーセキュリティ経営ガイドライン(経産省)
- 経団連サイバーセキュリティ経営宣言
- ISMS(JIS Q 27001(ISO/IEC 27001))

情報管理(秘密区分とITルールの連動)
- Three Lines Model(IIA(内部監査人協会))
- ISMS(JIS Q 27001(ISO/IEC 27001))
- NIST SP800-60(情報のセキュリティ分類)

社内IT(サイバーセキュリティ対策)
- ISMS(JIS Q 27001(ISO/IEC 27001))
- NIST CSF(Cyber Security Framework)
- NIST SP800-53, 171
- NIST SP800-207(ゼロトラスト)
- CMMC(Cybersecurity Maturity Model Certification)

サプライチェーン(約1,800社の点検・改善)
- ISO/IEC 27001, 28000
- NIST SP800-53, 171

お客様向けセキュリティ(セキュリティバイデザイン)
- Common Criteria (ISO/IEC 15408)
- PCI DSS(Payment Card Industry Data Security Standard)
- 政府機関の情報セキュリティ対策のための統一基準
- NIST SP800-53, 171

セキュリティ人材育成
- ITSS(ITスキル標準)

出典:NEC

３．セキュリティとトラストの関係

セキュリティとトラストの関係

■“セキュリティを高める”トラストのみならず、“セキュリティを担保した上でサイバー・フィジカル空間を含め闊達な利用促進を支える”トラスト

図2-1-3　セキュリティー・トラスト区分

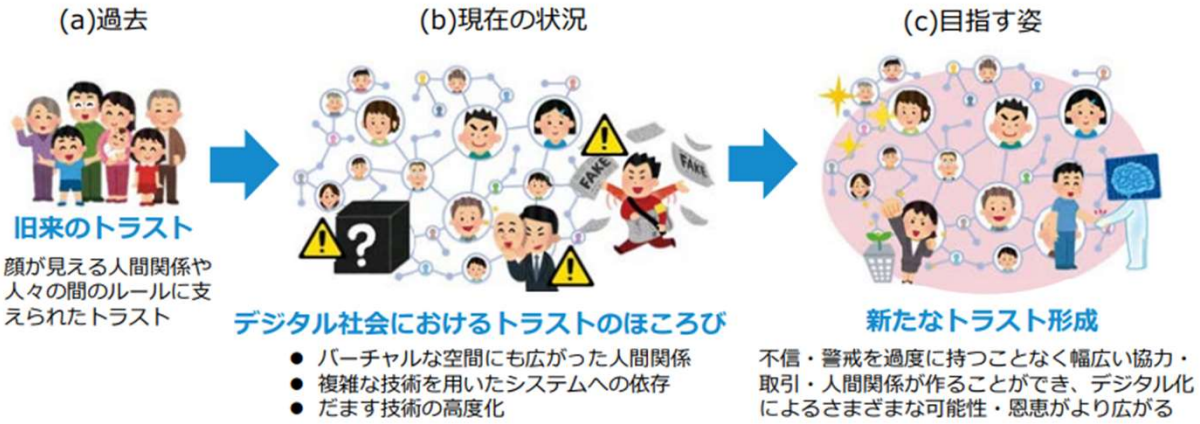


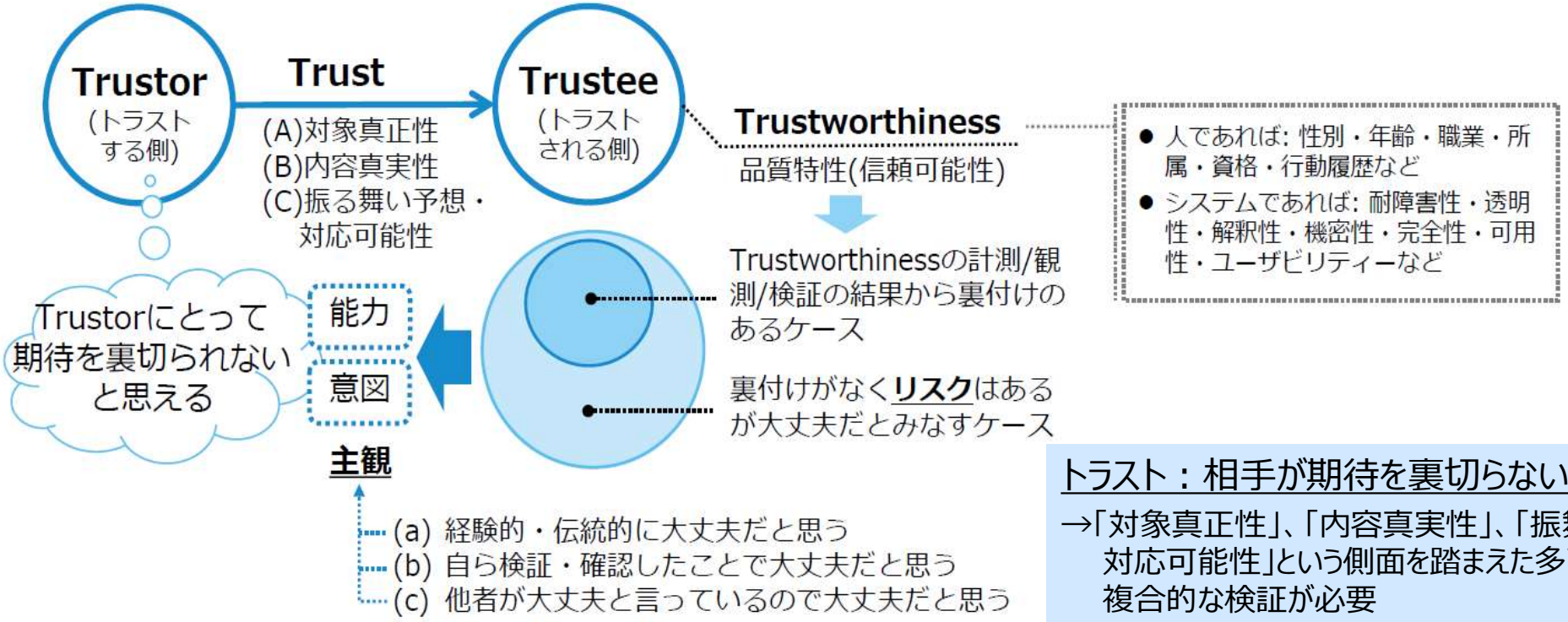
図1-1　デジタル社会におけるトラストの問題認識と目指す姿

出典：セキュリティー・トラスト分野の動向と今後の展望、デジタル社会における新たなトラスト形成（国立研究開発法人科学技術振興機構　研究開発戦略センター/CRDS)

トラストとは　– JST(*)報告書より –

(*) JST：国立研究開発法人科学技術振興機構

- 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

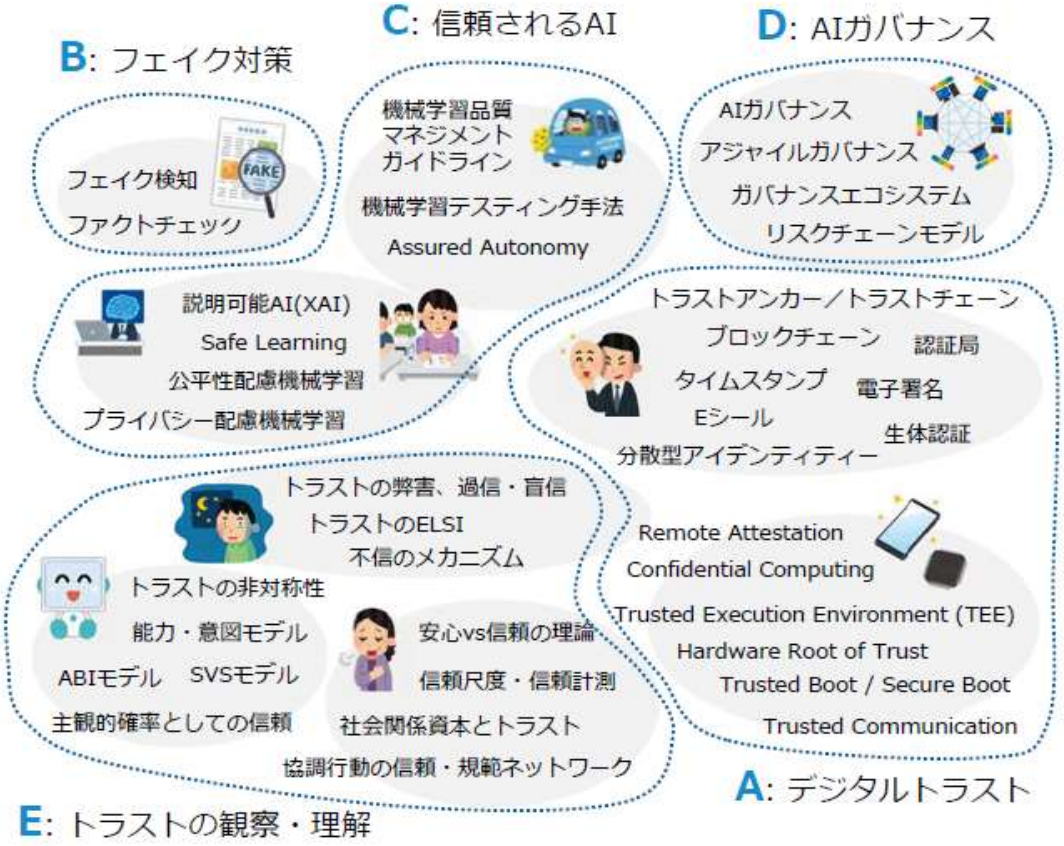


トラスト：相手が期待を裏切らないと思える状態

→「対象真正性」、「内容真実性」、「振舞い予想・対応可能性」という側面を踏まえた多面的・複合的な検証が必要

出典：デジタル社会における新たなトラスト形成 (https://www.jst.go.jp/crds/report/CRDS-FY2022-SP-03.html)

トラストを取り巻く環境
～ トラスト研究開発の観点の違い, そして分野横断での連携の必要性 ～



分類

- 技術開発による対策設計
  - 対象真正性の問題に重点 …… A: デジタルトラスト
  - 内容真実性の問題に重点 …… B: フェイク対策
  - 振る舞い予想・対応可能性の問題に重点 …… C: 信頼されるAI
- ルール整備・プロセス管理による対策設計 …… D: AIガバナンス
- 対策設計・社会受容の裏付け …… E: トラストの観察・理解

[注] おおまかな傾向であり、この見方に収まらない取り組みも存在する

[出典] デジタル社会における新たなトラスト形成 (研究開発戦略センター/CRDS)

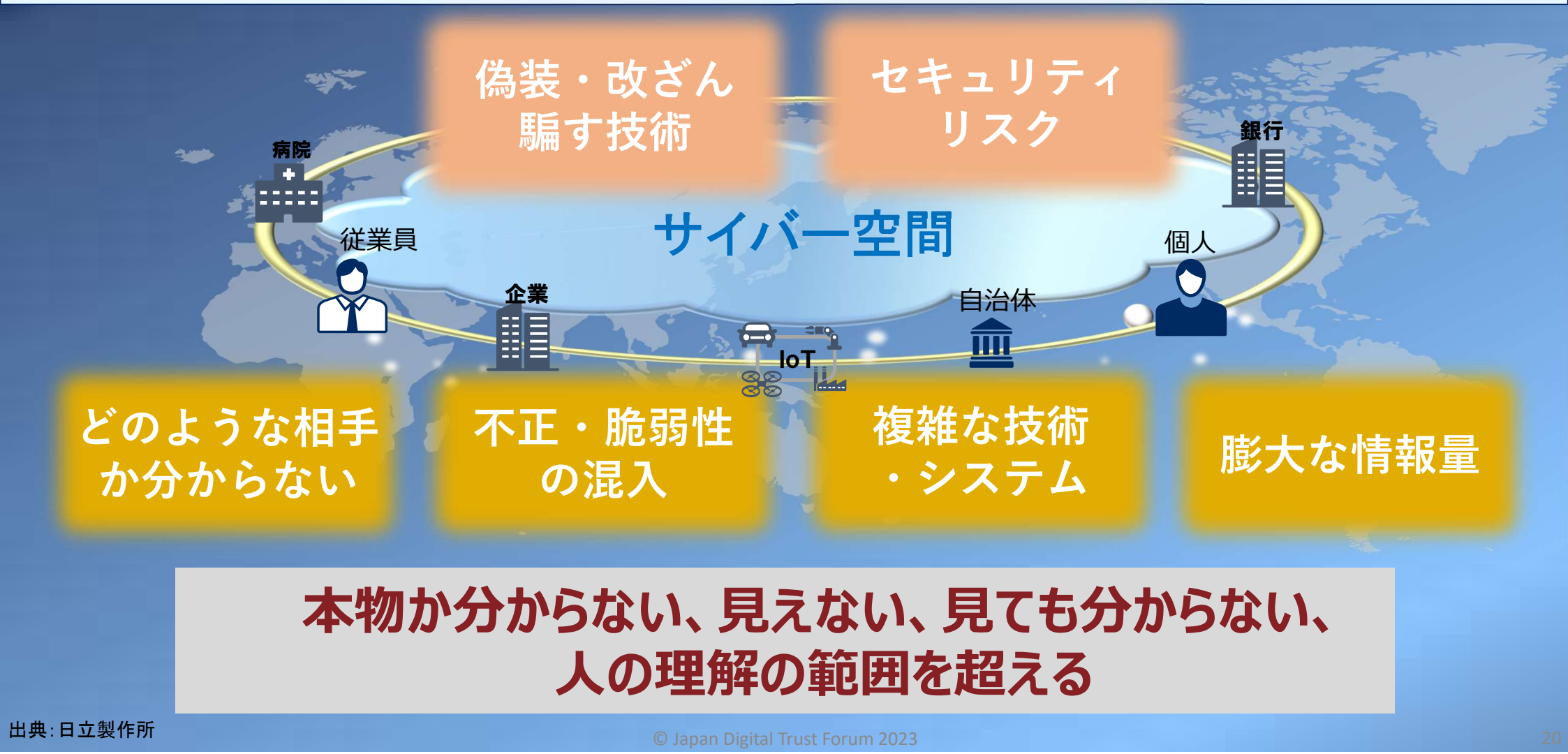
出典：デジタル社会における新たなトラスト形成 (https://www.jst.go.jp/crds/report/CRDS-FY2022-SP-03.html)

~ 注目されるトラスト関連政策提言・プログラム事例 ~

分類	国	政策提言・プログラム事例
A: デジタルトラスト	日本	「Data Free Flow with Trust (DFFT)」（2019年1月ダボス会議、安倍首相） ● デジタルトラスト協議会（2020年8月設立） ● 内閣デジタル市場競争本部 Trusted Web推進協議会「Trusted Webホワイトペーパーver.1」（2021年3月）、「同Ver.2（案）」（2022年7月） ● デジタルガバメント閣僚会議 データ戦略タスクフォース「包括的データ戦略」（2021年6月閣議決定） ● デジタル庁 データ推進戦略ワーキンググループ トラストを確保したDX推進サブワーキンググループ（2021年11月～）
	欧州	● eIDAS (electronic Identification and Authentication Service) 規則（2014年7月成立、2016年7月施行）：トラストサービスの統一基準
B: フェイク対策	米国	● 国防高等研究計画局（DARPA）「Media Forensics (MediFor)」プログラム、「Semantic Forensics (SemaFor)」プログラム
C: 信頼されるAI	日本	● 統合イノベーション戦略推進会議「AI戦略2019」（2019年6月）における主要な研究開発課題として「Trusted Quality AI」 ● 文部科学省2020年戦略目標「信頼されるAI」を受けたJSTプログラム：CREST「信頼されるAIシステム」、さきがけ「信頼されるAI」（2020年度～） ● NEDO「次世代人工知能・ロボット中核技術開発事業」において「AIの信頼性」（2020年度～）
	英国	● 英国研究・イノベーション機構（UKRI）「Trustworthy Autonomous Systems Programme」
D: AIガバナンス	日本	● 世界経済フォーラム「Rebuilding Trust and Governance: Towards DFFT」白書（2021年3月） ● 経済産業省「Governance Innovation Ver.2: アジャイル・ガバナンスのデザインと実装に向けて」（2021年7月）、「AI原則実践のためのガバナンス・ガイドライン Ver. 1.1」（2022年1月） ● 日本ディープラーニング協会「AIガバナンスとその評価」研究会報告書「AIガバナンス・エコシステム－産業構造を考慮に入れたAIの信頼性確保に向けて－」（2021年7月）
	欧州	● 欧州委員会「Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts」（2021年4月）

4．日本や欧州等におけるデータ流通、トラストに関する動向

- あらゆる組織、人、モノ、コト、価値がサイバー空間で繋がる、デジタルが介在する
- サイバー空間での繋がりの中で価値が交換され、社会、経済、産業の原動力になる



本物か分からない、見えない、見ても分からない、
人の理解の範囲を超える

出典：日立製作所

自国の安全・安心と競争優位性確保に向けたルール形成

見ても分からない ➡ 規程どおり実施していることの説明を求めるルール・規制

- ルールに則った適切なセキュリティマネジメント、脆弱性管理を実施しているか？
- 渡した機密情報（製造図面・ノウハウ、個人情報など）は、適切に管理されているか？

事業活動の正当性を説明できない

＝

経営リスク

出典：日立製作所

潮流　- 高まるサプライチェーンリスク -

新たなサプライチェーンリスクの広がり

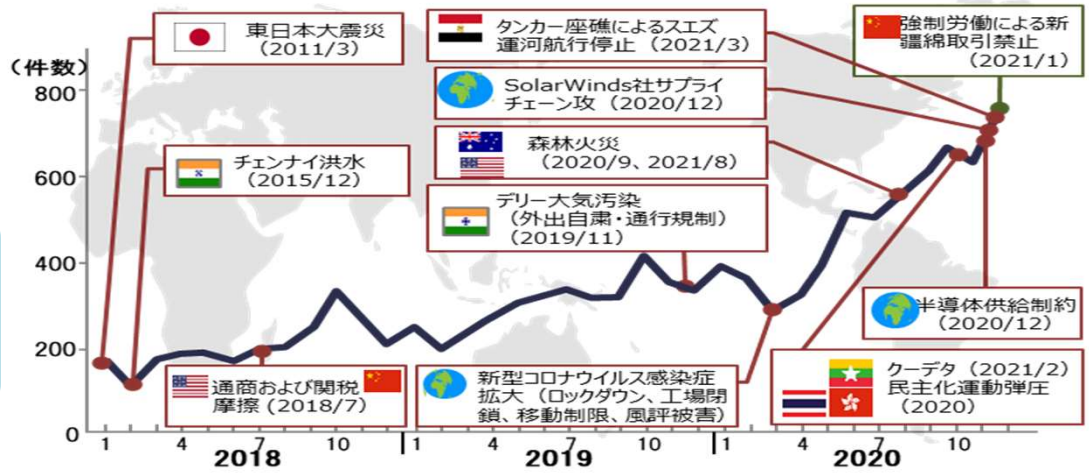
事業環境　…　サプライチェーンにおける管理範囲の拡大

- ✓ デジタル化、DXによるビジネスの急速な変化
- ✓ デジタル技術、不足リソースの調達先多様化・外部依存の高まり
- ✓ 取引のグローバル化、供給ルートの複雑化

社会環境　…　さまざまなリスクの顕在化

- ✓ 制御不能な外的要因によるさまざまなリスク顕在化

・地政学リスク：貿易摩擦、政治不安
・社会リスク　：人権問題、パンデミック
・環境リスク　：気候変動、脱炭素



潮流　- 経済安全保障推進法 -

DXの進展に伴い、競争力強化に向けた経済安全保障推進法が成立
基幹インフラ事業者やサプライヤーは対応を求められる

背景

国際情勢の複雑化、社会経済構造の変化等が進展する中、国民生活や経済活動に対するリスクが顕在化
- サプライチェーンの脆弱性により国民の生命・生活を脅かすリスクが顕在化
- 世界各国において、国家の関与が疑われるものも含め、サイバー攻撃により経済が大きく混乱する事例
- AI・量子などの技術革新、科学技術・イノベーションは、激化する国家間の覇権争いの中核に

対象分野

サプライチェーンの強靭化	基幹インフラの安全性・信頼性確保	先端技術開発	特許出願の非公開化
● 重要物資や原材料(例：半導体)のサプライチェーン強靭化	● **基幹インフラ機能の維持等に係る安全性・信頼性を確保**	● 官民連携し、技術情報を共有・活用し、重要技術を育成	● 特許非公開化の措置を講じて機微な発明の流出を防止

内容

制度の目的	基幹設備の事前審査制度	対象となる事業者・設備
・基幹インフラ設備導入等の際に事前にセキュリティリスク等を排除 ・重要設備の導入や維持管理等に係る委託状況やリスクを把握	・基幹インフラを担う設備の導入に際して、政府が事前審査を実施 ・設備の機能や設備の供給事業者や委託先の事業者に関する情報	・電力、ガス、水道、情報通信、金融、運輸、郵便、航空、鉄道等 ・設備、機器、装置、それらに係るプログラムまで対象が多岐にわたる

出典：経済安全保障法制に関する提言骨子
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai4/teigen.pdf

欧州サイバーレジリエンス法

デジタル製品の製造事業者に対し、製品に含まれる脆弱性とソフトウエアコンポーネントを特定・ 一覧化したSBOMの作成、製品ライフサイクル全体に対するセキュリティ要件への適合性証明等の義務化を検討中

EUサイバーレジリエンス法（草案）

- 2022年9月に草案提出。2023年後半の発効、**2025年後半の適用**を目指す。
- 例外を除き、**デジタル要素を備えた全ての製品が対象。SBOM作成や更新プログラム提供等セキュリティ要件への適合（自己適合宣言/第三者認証）が求められる。**
- **重要なデジタル製品について、低リスク製品でEUCCやEN規格対象外の製品は第三者認証を、高リスク製品には第三者認証を求める。**（中小企業の認証手続き減額
- 適合性評価証明書にはEU適合宣言書（CEマーク）/EUCC証明書を用いる。
- **脆弱性の悪用やインシデント発見後24時間以内にENISAへの報告を義務化。**
- **罰則あり。**（最高1,500万ユーロ又は当該企業の全世界売上高の2.5%以内）

注：EUCCとは、IoT製品を対象とする欧州サイバーセ
EN規格とは、欧州整合化規格

【対象】デジタル要素を備えた全ての製品

・デバイスやネットワークに直接的/間接的に接続されるものも含む。
・医療機器規則、体外診断用医療機器規則、民間航空機規則、自動車の型式承認規則の対象製品は適用除
・国家安全保障に関するデジタル製品や軍事目的・機密情報処理目的のものは除外。
・SaaSなどのソフトウェアサービスは対象外。研究開発目的のOSSなども対象外。

【適合性評価】使用環境等のリスクレベル毎に以下を求める。

- **「デジタル製品」 ・・・ 自己適合宣言か第三者認証を選択**
- **「重要なデジタル製品」のうちクラスI（低リスク）・・・EUCCやEN規格の対象外は第三者**
- **「重要なデジタル製品」のうちクラスII（高リスク）・・・第三者認証**

【適合性評価証明書】

・EU適合宣言書（CEマーク）に基づく証明書
・EUCCに基づく証明書（必要に応じてEUCCを必要とする製品を指定）
※この他、市場サーベイランスも行われる。
※第三国（日本も含む）との相互承認も可能。※条文上は見当たらず。

CEマーク

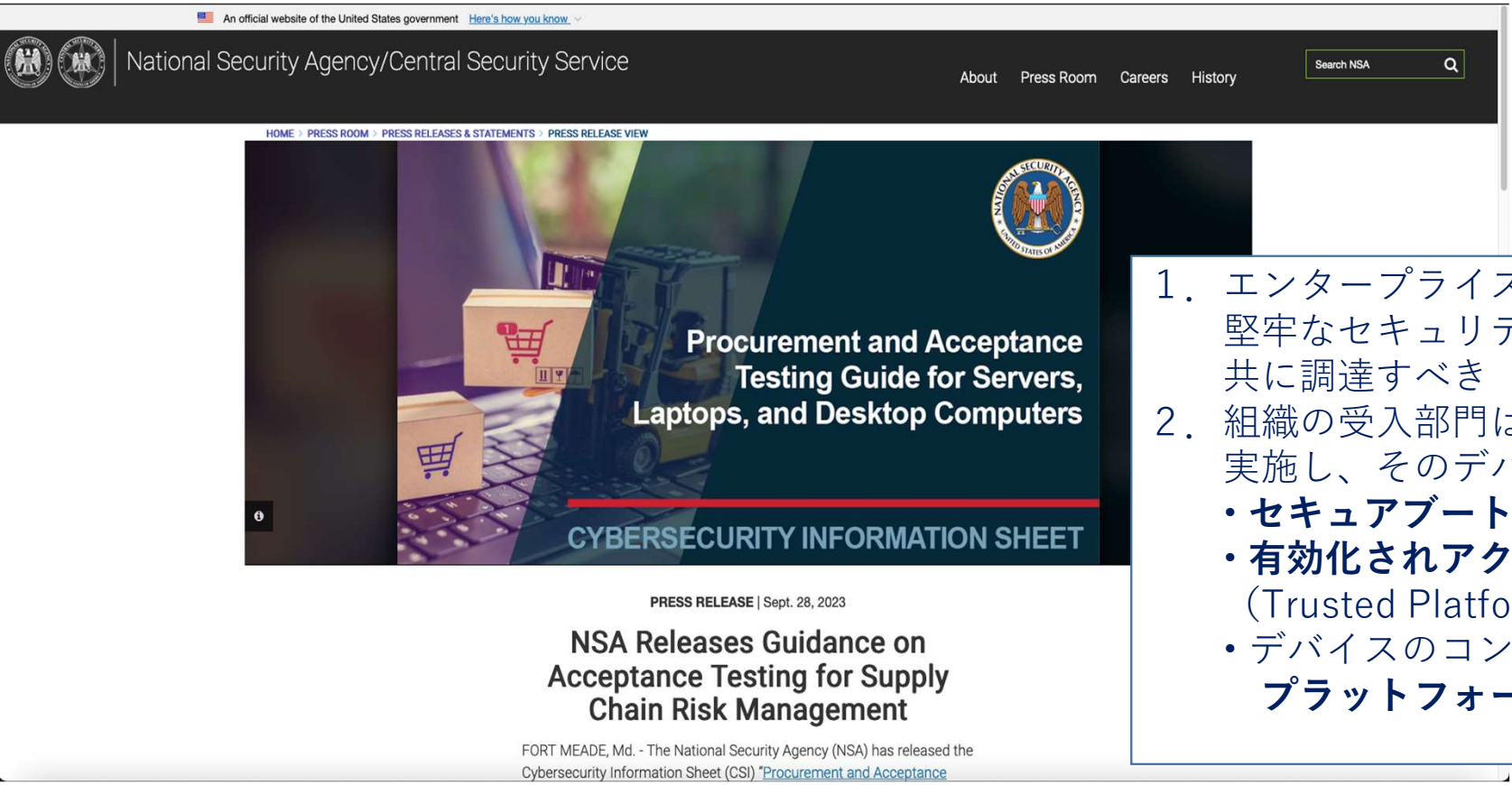
出典：CRAdraft.pdf (meta.go.jp)

製造業者の義務（10条）

① デジタル製品を市場に出す際、附属書Iの1**「セキュリティ特性要件」を遵守して**設計・開発・製造されていることを確認する。
② サイバーセキュリティ上の**リスクアセスメントを実施**し、その結果を設計・開発・製造・配送・メンテナンスの際の考慮に入れる。
③ デジタル製品を市場に出する際、上記のリスクアセスメントの結果を技術文書に含める。
④ 第三者から提供された部品を使用する際には、その部品により製品のセキュリティリスクを高めないことを保証する。
⑤ リスクに比例した方法でデジタル製品に関するサイバーセキュリティ側面を体系的に文書化する。
⑥ **上市後5年間**または製品寿命のうち短い期間の間、**脆弱性に効果的に対処**する。製造業者は脆弱性開示ポリシー等、適切なポリシーや手続きを有する。
⑦ 上市前に製造業者は**技術文書を作成**する。対応する適合性評価手続きを行い、適合性が実証された場合は**CEマーキングを貼付**する。
⑧ **上市後10年間、技術文書と（該当する場合は）EU適合性証明書を**市場監視当局が自由に使えるように**保管する。**
⑨ 一連の製造の中で、適合性を維持するための手順が整備されていることを確認する。
⑩ 附属書IIに規定される情報が製品に付属されていることを確認する。
⑪ EU適合性証明書を提供するか、その情報を記載したURLを提供する。
⑫ **上市後5年間**または製品寿命のうち短い期間の間、附属書Iの1**「セキュリティ特性要件」を遵守しない場合、直ちに必要な是正措置を講じ、製品の撤回またはリコールを行う。**
⑬ **市場監視当局からの要求**に応じて製品の**適合性を証明する情報・文書を提出**する。
⑭ 操業を停止し義務を遵守できなくなる場合、操業停止前に市場監視当局やユーザに通知する。
⑮ （欧州委員会は実施法の中で、SBOMの形式と要素を指定することができる。）

6

米国家安全保障局(NSA)：
サプライチェーンリスクのための調達、受入れ試験ガイダンスをリリース

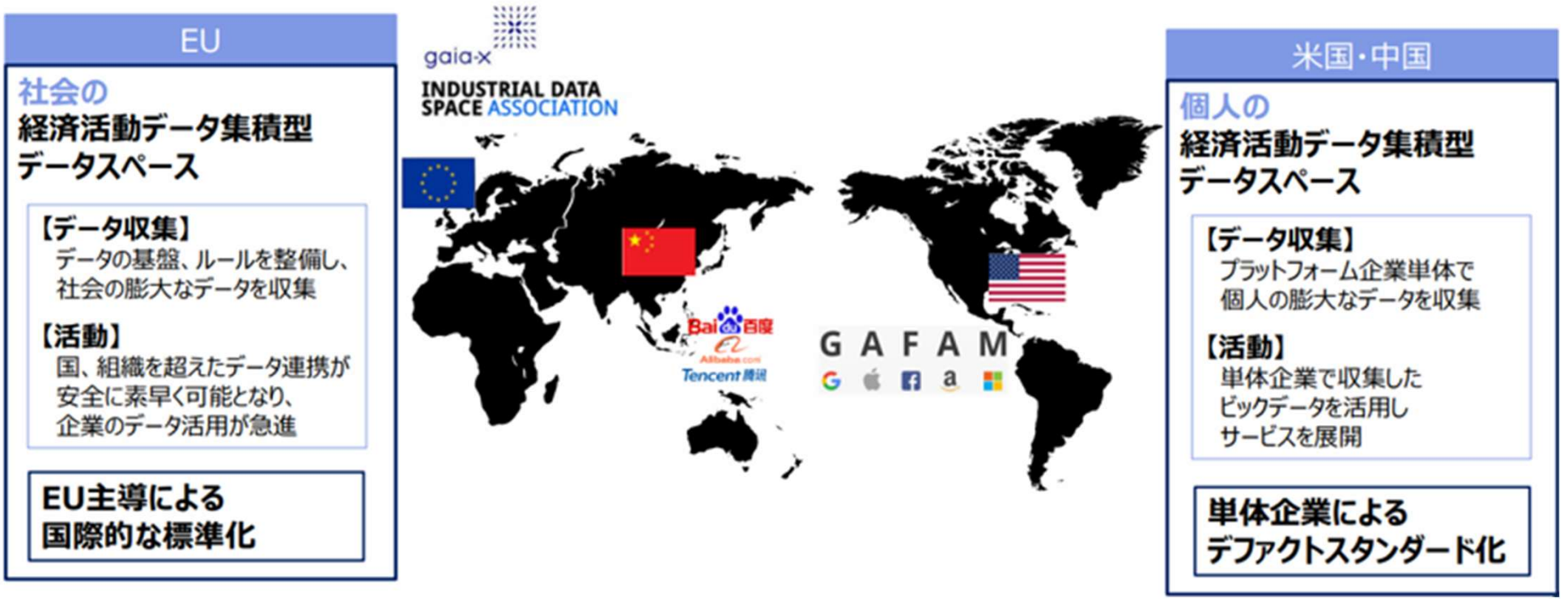


1．エンタープライズグレードのサーバ、PCは堅牢なセキュリティ成果物、構成、機能と共に調達すべき
2．組織の受入部門は自動化された受入検査を実施し、そのデバイスをチェックすべき
- **セキュアブート**が有効
- **有効化されアクティブ化されたTPM**（Trusted Platform Module）
- デバイスのコンポーネントと一致する有効な**プラットフォーム証明書**

出典：NSA：https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3541065/nsa-releases-guidance-on-acceptance-testing-for-supply-chain-risk-management/

データ流通、データスペースの動向

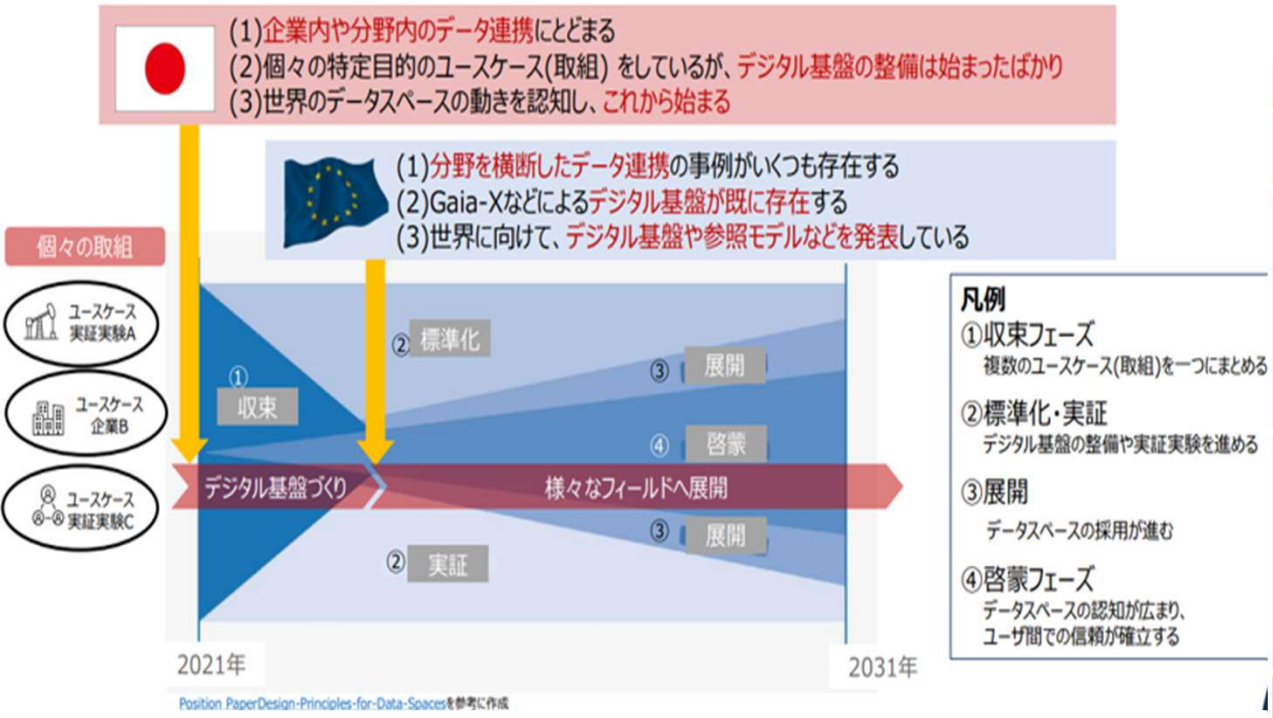
■EU・米国・中国はデジタル競争力強化のため、「データ」を活用しビジネスを展開



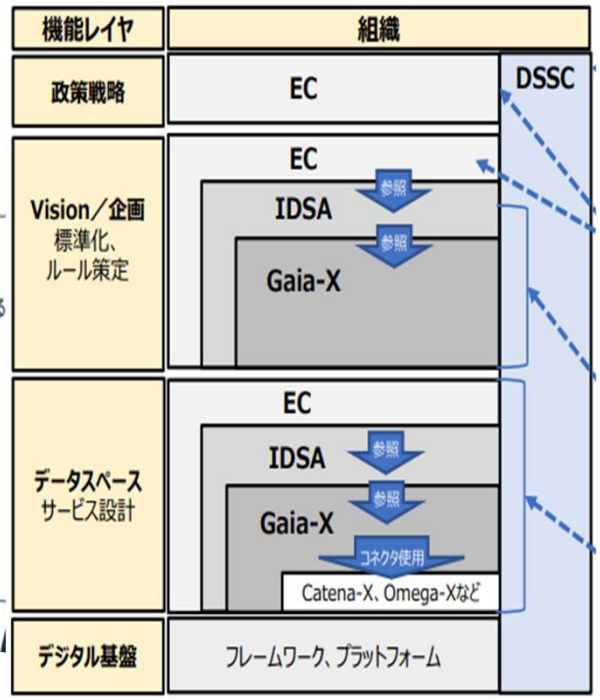
出典：IPA、データスペース入門（https://www.ipa.go.jp/digital/data/jod03a000000a82y-att/dataspaces-gb.pdf）

EUと日本のデータスペースアプローチ

■EUは体系的に取組をすすめていて、日本よりはるかにスピードがはやい



■ EC、IDSA、Gaia-Xの各組織で設計方針を参照し、データスペース間の接続手順を統一



DSSC
(Data Spaces Support Centre)
ﾚｲﾔ縦断でﾃﾞｰﾀｽﾍﾟｰｽ参加者の支援を行う組織
(EU, ISDA, Gaia-X共同出資)

欧州委員会(EC)
・2018年 GDPR施行
・2020年「欧州ﾃﾞｰﾀ戦略」発表
「欧州ﾃﾞｰﾀｽﾍﾟｰｽの構築により、産業用ﾃﾞｰﾀの有効活用を通じてEU発展を目指す

IDSA：
・技術仕様ﾘﾌｧﾚﾝｽ・ｱｰｷﾃｸﾁｬ(RA)を策定

Gaia-X：
・IDSAのRAを参照し、Gaia-XのRF策定

欧州委員会(EC)：
・ﾃﾞｰﾀｽﾍﾟｰｽの基本ﾊﾟｰﾂを作成

IDSA：
・IDSｺﾈｸﾀ*を作成

Gaia-X：
・IDSｸﾈｸﾀをｺｱ技術にEclipseｺﾈｸﾀを開発し、Catena-X等のﾃﾞｰﾀｽﾍﾟｰｽで使用

＊ｺﾈｸﾀ：ﾃﾞｰﾀｽﾍﾟｰｽ間でﾃﾞｰﾀ連携を行う仕組み

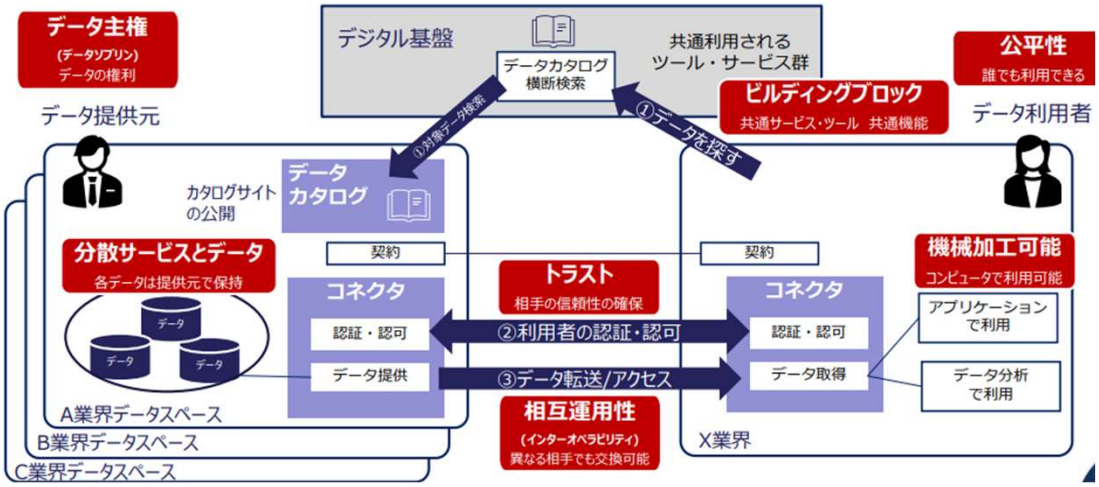
出典：IPA、データスペース入門を元に作成
（https://www.ipa.go.jp/digital/data/jod03a000000a82y-att/dataspaces-gb.pdf）

データスペース及びスペース間の連携においても、やはりトラストが必要

■データスペースのデータ連携は、主に、

①データを探す、②認証・認可、③データ転送/アクセスの３ステップ。

■「相互運用性」、「データ主権」がデータスペースで重要



■データスペースの対象領域

・社会の幅広い分野でデータスペースが推進されている。

・日本は、データスペースと呼んでいないが、準公共プロジェクトなどデータスペースに類似の取り組みが数多く行われている

日本標準産業 大分類	EU	日本
A 農業，林業	EDS農業	準公共（農業）
B 漁業	漁業	
C 鉱業，採石業，砂利採取業		
D 建設業	EDS建設	スマートビル、地下埋設物 国土交通PF
E 製造業	EDS産業・工業、モビリティ	企業間取引、蓄電池
F 電気・ガス・熱供給・水道業	EDSエネルギ	水道
G 情報通信業	EDSメディア	
H 運輸業，郵便業	EDS鉄道、モビリティ、 航空、海運	自律移動ロボット モビリティ（サービス）
I 卸売業，小売業		
J 金融業，保険業	EDS金融	金融
K 不動産業，物品賃貸業		国土交通PF
L 学術研究，専門・技術サービス業	EDS文化遺産	
M 宿泊業，飲食サービス業	EDSツーリズム	
N 生活関連サービス業，娯楽業	EDSツーリズム	
O 教育，学習支援業	EDSスキル	準公共（教育）
P 医療，福祉	EDSヘルス	準公共（医療）
Q 複合サービス事業	EDSスマートコミュニティ	準公共（スマートシティ）
R サービス業（他に分類されないもの）		
S 公務（他に分類されるものを除く）	EDS行政、 行政(法、調達、安全)	公的個人認証 公共サービスメッシュ 準公共（防災）
T 分類不能の産業	EDSグリーンディール	CFP カーボンフットプリント

＊EDS：欧州のデータ戦略で推進されるEurope Data Space

出典：IPA、データスペース入門（https://www.ipa.go.jp/digital/data/jod03a000000a82y-att/dataspaces-gb.pdf）

関係府省庁、DSA、IPAがOne Teamで推進

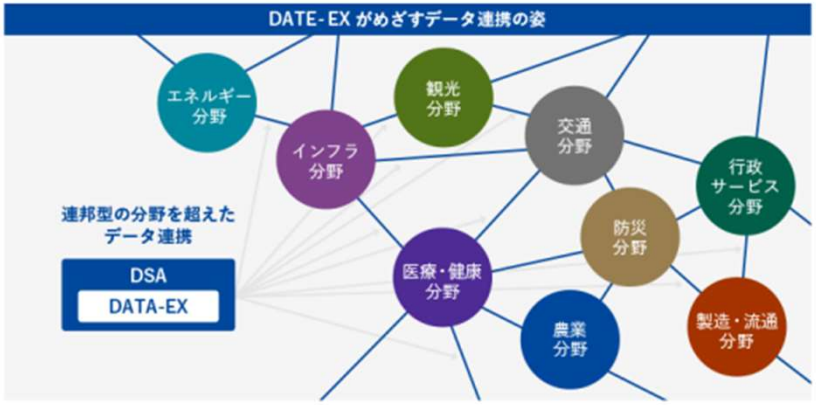
One Team
- 経済産業省
- デジタル庁
- 関係府省
- 情報処理推進機構（IPA）※
- 国立印刷局※
- 地方公共団体情報システム機構（J-LIS）※
- 情報通信研究機構（NICT）※
- データ社会推進協議会（DSA）

・・・

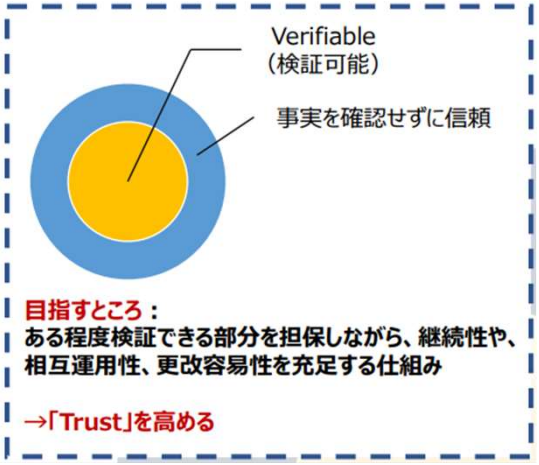
※デジタル社会の実現に向けた重点計画で連携強化と記載

第３期SIP サーキュラーエコノミーシステム

一般社団法人データ社会推進協議会
DATA-EX
Data Society Alliance



Trusted Web推進協議会



出典：IPA、データスペース入門等を元に作成

５．具体的な社会課題と手段としてのトラストサービス

デジタルトラスト

DXの恩恵を享受する為、サイバーフィジカル空間のトラスト形成を迅速化・容易化
- **対象真正性(注)：本人・本物か、データの完全性、人、組織、モノの実在性を確認可能**
- **内容真実性(注)：内容が事実、真実であるか確認可能**
- **リスク評価　　：信頼する側が、属性などにより、リスクやその対応性を評価可能**

(注)以下を参考に作成
デジタル社会における新たなトラスト形成 (https://www.jst.go.jp/crds/report/CRDS-FY2022-SP-03.html)

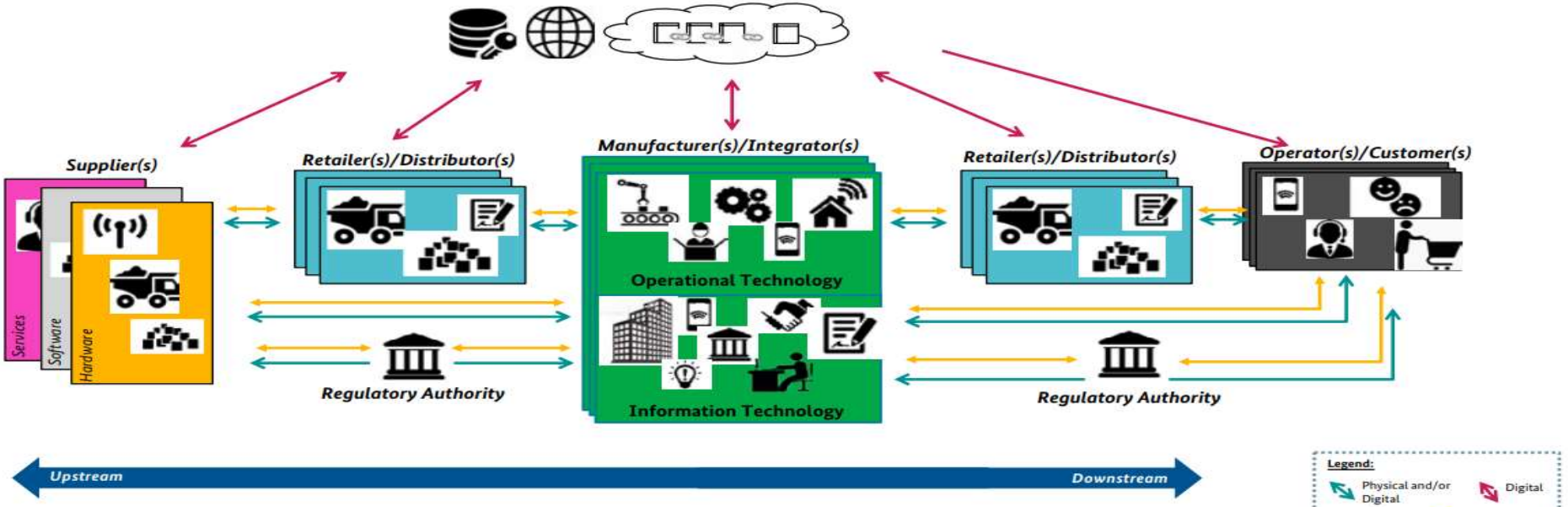
Traditional Trust
(1)現場、現物、書面による確認
　→当事者の確認結果の書面確認含む
(2)人手、時間、コストをかけて確認
(3)取引先との間で個別に確認
(4)時間がかかる、スケーラビリティ小
(5)監査などの定点記録

Digital Trust
(1)第三者による検証可能性
　(対象真正性、内容真正性、リスク)
(2)リモートで迅速に容易に確認
(3)バリューチェン全体で確認
(4)高速処理、スケーラビリティ大
(5)事後検証、検索可能

→サイバーフィジカル空間におけるトラストのインターオペラビリティの確立により可能となる。

1）サプライチェーンにおけるデジタルトラスト

サプライチェーンの信頼性、リスクを、サプライチェーン全体で評価、検証可能な仕組み



出典： https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/IIoT_Value_Chain_Security2.html

(1) サプライチェーンで創出された価値(製品・サービスなど)が期待どおりであること
(2) サプライチェーンにおける価値の創出過程が期待どおりであること
(3) 価値がアフターサービスも含めて期待どおり提供され続けること

参考.　ESG投資における想定課題

■EUは、**サプライチェーン全体での環境・人権への取り組みを評価するためのルール・規制強化**
　→Scope3も含めた排出量の**正確な把握、第三者認証に基づく開示**などを検討中
■CO2排出量取引、M&AのDDなど、今後、**排出量の担保だけでなく、説明責任が問われる可能性**

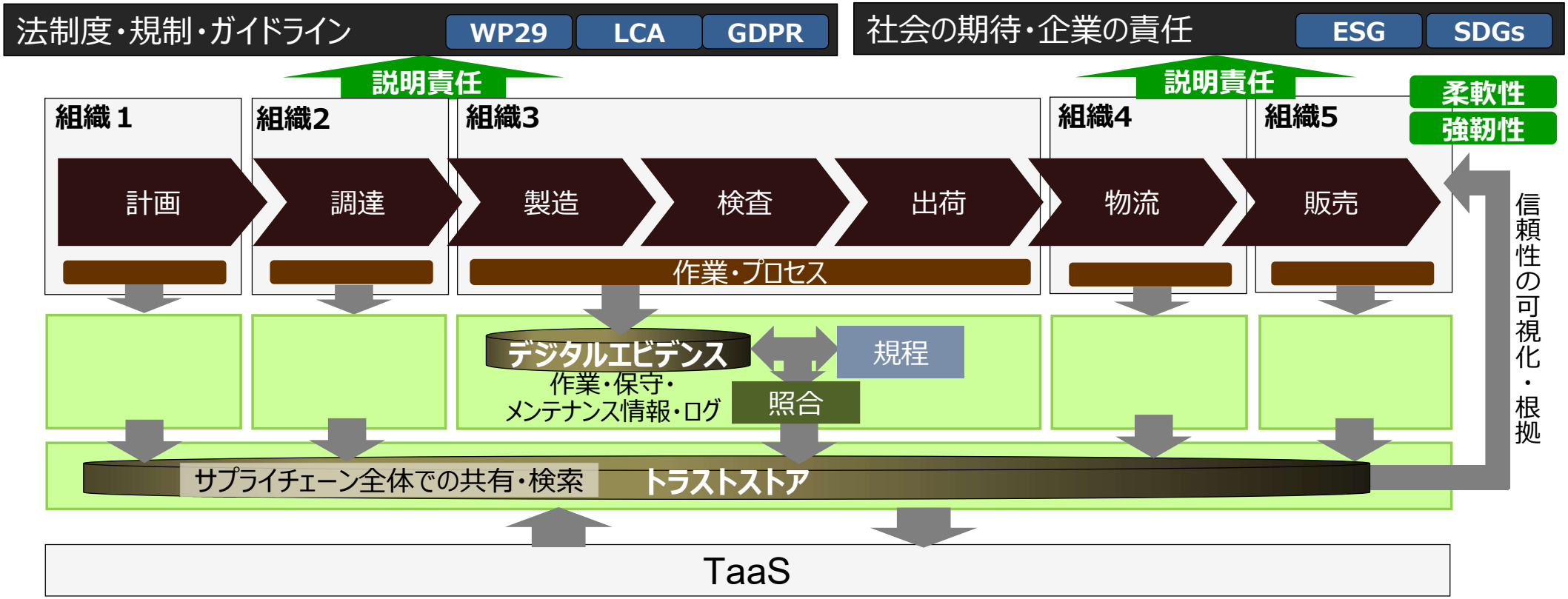
ステークホルダ	想定課題
金融機関	・ESGに関するインパクト評価が求められるが、財務情報以外の知見に乏しい、収集が大変。 ・開示情報の信憑性、不正リスク（グリーンウォッシュ）
機関投資家	・投資による社会貢献効果が不明瞭 ・開示情報の信憑性、不正リスク（グリーンウォッシュ）
事業会社	・脱炭素の投資目的に関する情報開示などの業務負担大。
監査法人	・非財務系監査におけるルール不足→非財務系は収集項目、ルール等のコンセンサスがない ・レギュレーター、投資家、市場の要請への対応力。

課題

- **DX、デジタル技術による効率化、対応力の強化**
- **価値交換（CO2排出量取引など）におけるトラスト確保**

実現イメージ

- サプライチェーン全体での**不正混入防止、製品・サービス要件への準拠/対応**
- サプライチェーンの信頼性を可視化し、**組織、人、価値の繋がりの柔軟性、強靭性確保**　柔軟性　強靭性
- 生産活動、事業活動における**エビデンス提示の要求、透明性確保、義務化への対応**　説明責任



2）デジタルアイデンティティにおけるデジタルトラスト

- W3CでのDIDs・VCsやEUでのDIWなど新たなIDの管理に対する取り組みが進んでいる
- 国内においても、新たなweb技術を使用したトラストの技術・アーキテクチャ・プロトコルなどの開発をユースケースの社会実装までを含めて、Trusted Webとして推進している。
- 一方、（わが国では）信頼あるデジタルID プロバイダーの在り方の議論がされていない。これら技術を活用していくうえで、認証局などのトラステッドサービスやベースレジストリとの連携など、実社会の商習慣や法制度との整合性を踏まえた実用化に向け、パブリックトラストの実現に向けた検討が必要。

DIDs/VCsの技術調査

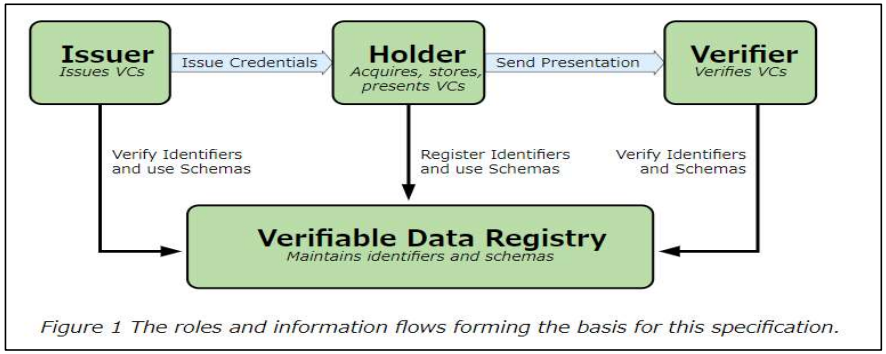
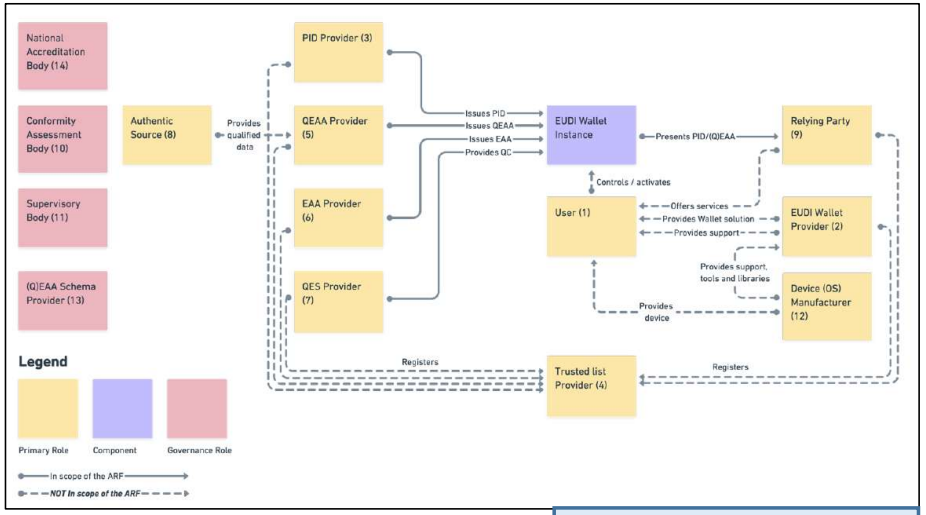


Figure 1 The roles and information flows forming the basis for this specification.

参考）W3C

EUDIW(EU Digital Identity Wallet)の技術調査



参考）ARF (v1.0.0) [2023/02]

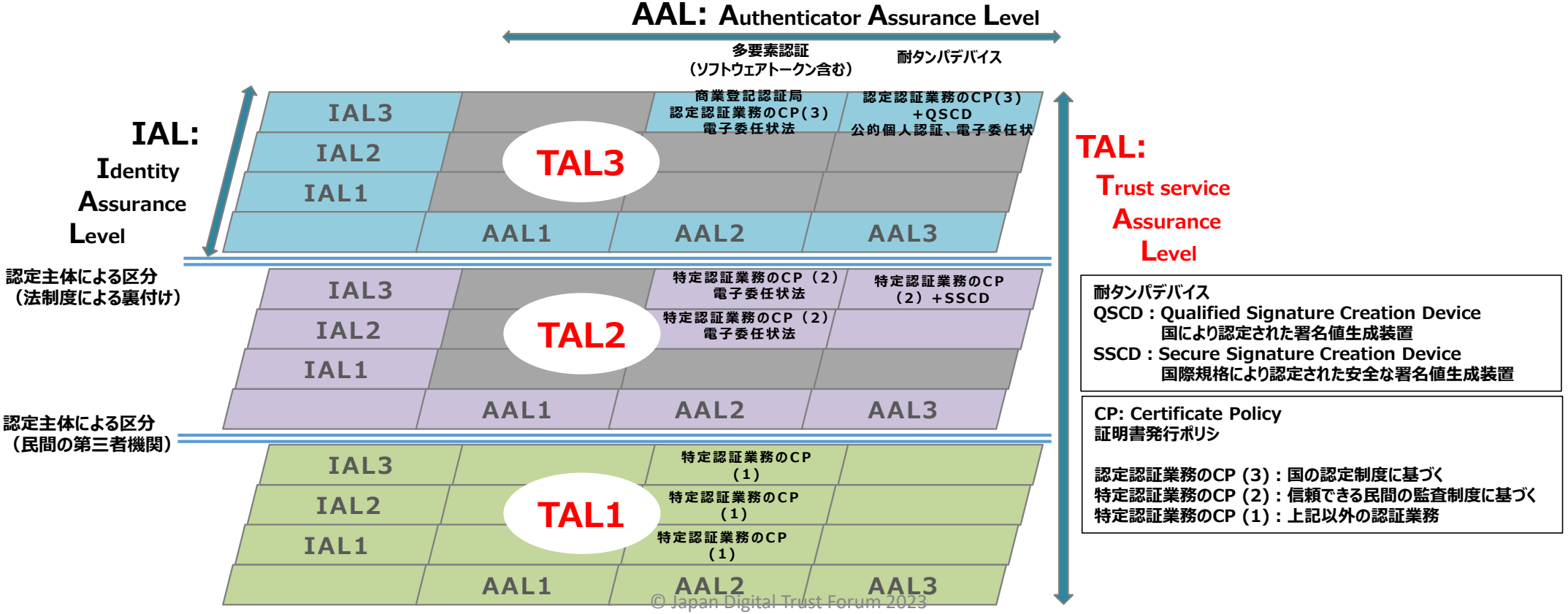
アシュアランスレベルの基準(IAL,AALに加えTALの提案)

◆ これまで議論されてきたIAL,AAL等に加え、IDを提供するProviderにもトラストサービスとして運営する際のAssurance Level(TAL)の定義とレベル分けが必要

しかしながら、eID ProviderのTALにはIAL,AALを要件に含むと考えられる⇒組み合わせが限定される

例）TAL＝3の必要要件として、IAL=3かつ、AAL ≧ 2かつ、BAL、InfoALが高い？ベースレジストリとの継続的な整合性を維持することが含まれる

例）TAL＝2の必要要件として、IAL≧2かつ、AAL ≧ 2かつ、BAL、InfoALが高い？として機能することが含まれる



耐タンパデバイス
QSCD : Qualified Signature Creation Device
国により認定された署名値生成装置
SSCD : Secure Signature Creation Device
国際規格により認定された安全な署名値生成装置

CP: Certificate Policy
証明書発行ポリシ

認定認証業務のCP (3)：国の認定制度に基づく
特定認証業務のCP (2)：信頼できる民間の監査制度に基づく
特定認証業務のCP (1)：上記以外の認証業務

3）ビジネスプロセスにおけるデジタルトラスト

ビジネス領域で行われてきた書面・押印・対面により信頼を確保してきた業務プロセスは、
DXによる利便性を享受するためには、従来とは異なる方法で流通する情報の信頼性を確保する必要がある。
→業務プロセスにおける、デジタル情報の流通において、利用者視点で、業務効率化を図りつつ
　　信頼性を確保するための課題を抽出し、解決策としてのトラストサービス利用を検討。

- 法人本人確認検討WG
  - 課題：金融取引時の法人本人確認業務における実印・印鑑証明書等の現物媒体の利用
  - Goal：法人本人確認のデジタル化実現による企業と金融機関双方の業務効率化
- 行政手続研究TF
  - 課題：行政への各種申請手続きはオンライン化が進むものの、申請に対する処分通知（許可証等）はオンライン化が進んでいない。
    　　そのため、受領側での人手作業負荷が高く、また、誤入力リスクの低減が困難。
  - Goal：「行政のデジタル完結」の方針のもと、処分通知等の受領側のプロセスを調査／分析し、あるべき姿を検討し行政への提言案を作る。
- ｅシール利用者ガイドラインTF
  - 課題：ｅシール用証明書の制度検討が進む中、ｅシールを利用する企業側において管理規程がない。
  - Goal：ｅシールを利用する企業側のガバナンス指針を具体的に示すガイドラインを策定・公開する。

具体的な事例：法人本人確認

- 「法人本人確認検討ＷＧ」での検討
  - 銀行業務（口座開設・融資申込）をモデルに、法人の本人特定事項をデジタル上で行なう仕組みについて検討

デジタル化を阻害する原因	解決方針
①法人が本人確認用書類を取得するデジタル上の仕組みがない	解決方針① **・実印＋印鑑証明書等に代わる、法人の証明(電子証明書)をデジタル上で付与できる仕組みの構築** **・登記情報の更新等をデジタル上で行う仕組みの構築**
②銀行へ提出された本人確認用書類を用いて、銀行がデジタル上で本人確認を行う仕組みがない	解決方針② **・電子証明書の真正性、法人情報*、委任情報等の照会を、デジタル上で行う仕組みの構築** *登記情報、定款、決算情報等
③代表者本人以外が申請を行う場合、銀行が申請者の法人の所属・権限有無がわかる仕組みがない	解決方針③ **・個人が所属している法人情報をデジタル上で照会する仕組みの構築** **・法人代表者から個人へ権限委任をデジタル上で登録・照会する仕組みの構築**
④各銀行単位で、全ての認証業務を行っており、業務の重複が発生（企業側もサービスごとに都度対応が必要）	解決方針④ **・法人の証明書、法人情報、委任情報、個人の所属情報等を一元的に管理し、真正性を担保する基盤の構築**

4）DFFTを支える国際相互承認の必要性

■国際社会での「信頼ある自由なデータ流通：Data Free Flow with Trust」の拡大

Society5.0の実現に向け、ヒト、モノ、システム間での高度な情報連携が進みAI含めデータの自動連携が社会システムの基盤となり、デジタル経済を支える**信頼ある自由なデータ流通（DFFT）が国際社会の中で拡大することが予想**されている。
「デジタル社会の実現に向けた重点計画」（R4年6月18日閣議決定）の「包括的データ戦略」では、「**データ流通に関連する国際的なルール作りや討議等を通じて、DFFT を推進し続ける必要がある。**」と示されている。

■DFFTを支えるトラストサービスの国際相互承認の必要性

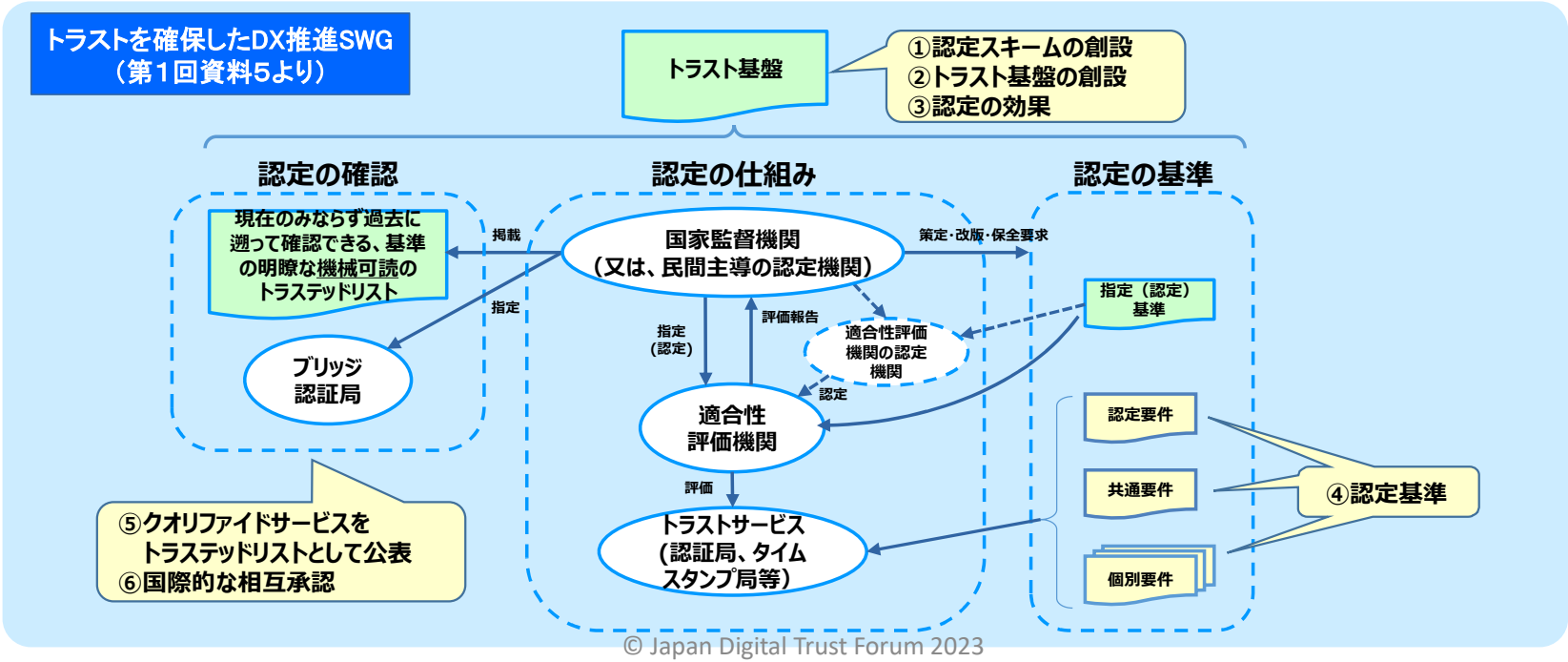
「包括的データ戦略」では、**データのトラストの3要素**「意思表示の証明(電子署名等）」、「 発行元証明（eシール等）」、「存在証明(タイムスタンプ等）」の国際的な相互承認の必要性について、「国際的な相互承認を得るにあたっては、トラストアンカーの確認、**トラストアンカー間の接続の仕組み**、及び **技術基準の整合性の確保**のみならず、**監督・適合性評価のレベル**や関連の**国内制度の整合性も確認**する必要性 が想定される。このため、国内のトラストサービス認定のフレームワーク では、**国際的な同等性等を配慮した国際相互承認を検討段階から 念頭に置くことが必要である。**」と述べられている。

包括的データ戦略で示された、トラストを確保する枠組みの実現に向けた検討を加速する必要がある

■わが国のトラストサービスは国際的な通用性に課題あり

電子署名を例にとると、残念ながら、日本の電子署名法の認定基準を満たした電子証明書は、国際的な通用性は無く、例えばPDFに署名された文書を受け取りAdobe社の”READER“で開いても直ちには電子署名の有効性が確認できず、手動で当該認証局を信じるという操作を行うことを余儀なくされる。これは**欧州や北米の技術標準とのマッピングがされていない**ため、**わが国の電子署名が国際的に認知されていない**ことを意味する。諸外国と電子署名データをやり取りする際はもちろんのこと、**READERのようなグローバルなソフトウェアを日本で利用する際にも課題**がある。**国を超えた電子署名の通用性を確保する上でトラストービスの国際相互承認が不可欠となる**。このことは、現在総務省で検討されている「eシール」についても同様である。

トラストサービスの国際相互承認に向け以下の①～⑥の論点に従ってトラストを確保する枠組みの整備の具体化に向けた検討を加速すべき



トラストサービス全般に関わる包括的な基準：

- 例えば欧州ではeIDASという包括的な上位の法の下、トラストサービスが定義され、下位の法制度や標準規格、認証基準等が構造的に整備されている。一方、我が国では包括的な体系がなく、トラストサービスの一部である電子署名とタイムスタンプに関わる法制度がそれぞれ独立して規定されており、互いに統一が取れているとはいいがたい状況にある。

法令等と技術標準との分離：

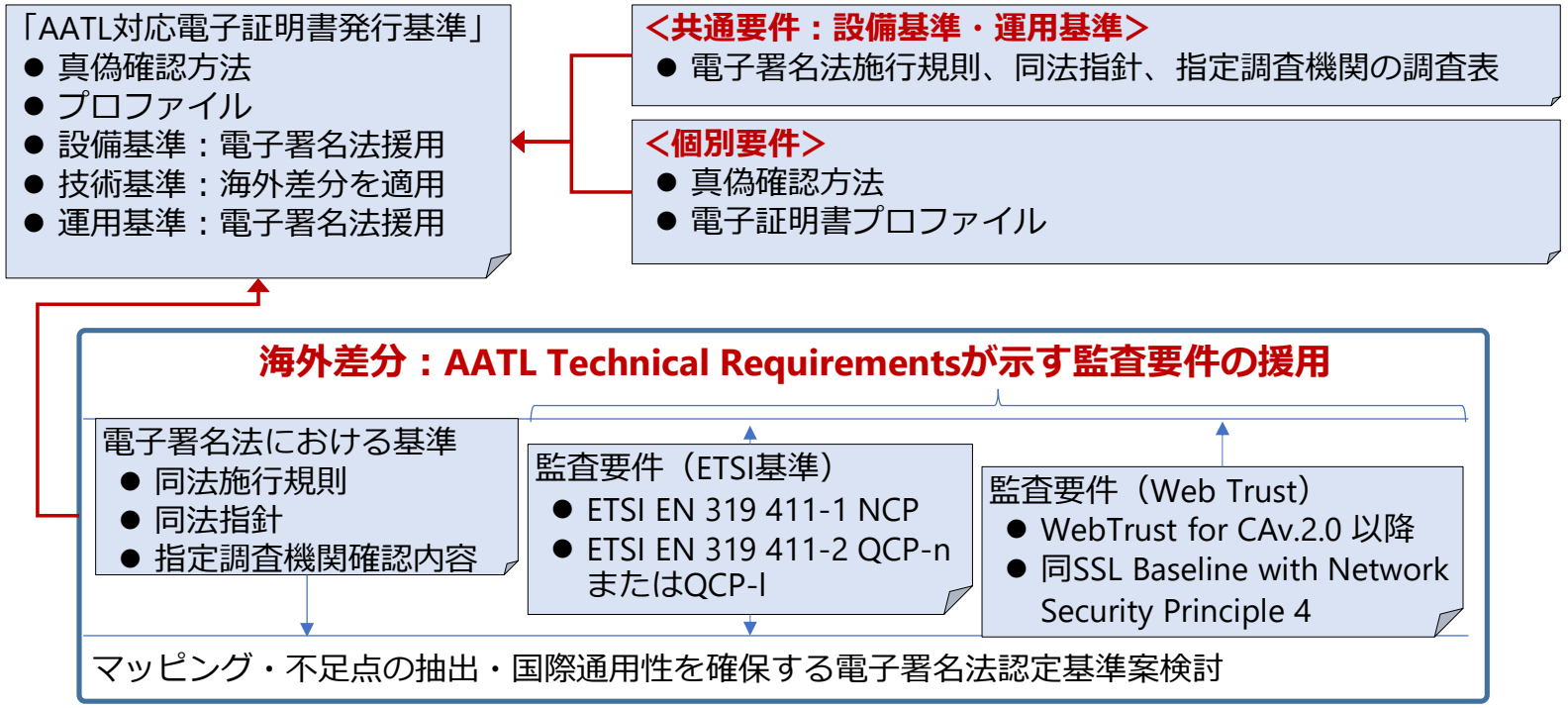
- 欧米では法令等と技術標準とは、ドキュメントとしても作成に当たる体制としても分離され、両者を関連付ける規則を設けて統制をおこなっている。一方、我が国では、例えば電子署名やタイムスタンプ関連では、法令等に技術基準の要素が含まれており、ドキュメント体系、作成にあたる体制ともに混在している。そのため、更新や見直しのタイミングも、担当すべき専門家も本来異なるため、更新の遅れや規定の不備、作業効率やコストへの悪影響をはじめとする問題の誘引が予見される。

未整備のトラストサービスの技術基準等の調査：

- 我が国で制度化されている電子署名やタイムスタンプ以外に、欧州等ではTSP評価機関、認証局、タイムスタンプ局、リモート署名、署名検証、身元確認、長期保存、eデリバリー等の技術基準が策定されている。

具体的な事例：AATL認証

- EUではETSI基準を満たせばAdobeで信頼済みソースとして自動的に検証が可能
- 電子署名法を満たすとAdobe基準も同時に満たすような「電子署名法のモダナイゼーション」に向け準備を進めている。



具体的な事例

- 電子帳簿保存法対応：
  - データの真実性確保の要件の１つとしてタイムスタンプが挙げられているが、その利用意義や注意事項、運用上の疑問・不安点に対する正しい知識、タイムスタンプ以外で運用する場合の注意事項等について、市場の理解に齟齬が見られる。
- 知的財産保護：
  - 特許庁による先使用権制度事例集において、タイムスタンプや電子署名について紹介されたものの、それらの具体的な利用方法や必要なツールの種類等に関する認知が広まっていない。
- 当協議会の活動・最新動向の広報：
  - デジタルトラスト自体の理解促進や、今後普及が予想されるeシールに関する動向等に関して、包括的に整理された情報が公開されていない。

6. まとめ

まとめ

1．サイバー空間の経済活動を狙った脅威が増大し、会社存続を脅かすインシデントが多発
2．デジタル社会に向けた『説明責任』を課すルール形成が加速し、
　企業にとって新たな経営リスクが増大
3．DXの恩恵を十分に享受するため、サイバー・フィジカル空間における
　トラスト形成の迅速化・容易化を推進すべき
4．デジタルトラスト実現に向けて、国際通用性を踏まえた普及へのルール作りが重要

→トラストを確保することは経営における説明責任を果たすためにも重要！
CIO/CISOの皆様にとって、安全を確保するセキュリティだけでなく、信頼を確保するトラストへの対応も必須！
→信頼性と自由なデータ流通の普及には産業界で協力することがとても大切！
→並行して、個社でデータ利活用に向けた整備を加速！

是非ともデジタルトラスト協議会にご参加いただきたい！
（https://jdtf.or.jp）