ID	No	提出者	該当箇所	御意見	御意見に対する考え方
1	1	個人	-	(意見を要約) 今後、「センサー技術、ネットワーク技術、デバイス技術」から成る「CPS（サイバーフィジカルシステム）」の導入により、「ゼネコン（土木及び建築）、船舶、鉄道、航空機、自動車、産業機器、家電」等が融合される構造へと変化します。かかる環境では、「検知（ディテクション）⇒分析（アナライズ）⇒対処（リアクションメソッド）」での「サイバーセキュリティー対策」が重要と考えます。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
1	2	個人	-	(意見を要約) 情報処理技術者試験の在り方について，経済産業省においては「国家資格ではなく、能力を認定する国家試験」と回答しているが、抜本的に再検討するのであれば、名称独占型の国家資格として技術者個人の職業的地位を保障すべきではないか。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
1	3	個人	-	(意見を要約) 社会福祉法人東京コロニー・職能開発室から独立行政法人情報処理推進機構（IPA）に対し，障害を理由とする差別の解消の推進に関する対応要領，情報処理技術者試験に関する合理的配慮の具体例として意見提出されている。未だ実現されていないものが多く，重度障がい者にとって就労につながるITスキルの証明であるCBT方式のITパスポート試験，基本情報技術者試験，情報セキュリティマネジメント試験の受験において「障害者差別解消法に基づいた合理的配慮」を国家の責務として講じてもらいたい。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
1	4	個人	-	(意見を要約) 2001年、通商産業省による国家プロジェクトの一環として設立されたITコーディネータ資格制度について、以下の理由により、経済産業省の推進資格としての位置付けではなく、その認定試験等の実施を独立行政法人情報処理推進機構IPAが行う、情報処理技術者試験に加えることを提案いたします。 ・認定試験がCBT方式で実施されている。 ・ITを利活用する側の人材にとって認定試験の難易度がITパスポート試験からのキャリアパスを鑑みたとき、無理のない適切な難易度であると思慮できる。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
2	1	団体	-	日本システムアドミニストレータ連絡会(JSDG)は、業務部門とITを一体にして業務改革プロジェクトを成功に導くキーパーソンとして進化しようとし続けている「シスアド」たちの集団です。 私たちシステムアドミニストレータは、業務改革を推進するリーダーとして、利用者の視点でITの活用を促進し、社会の発展に寄与する存在であり続けることを、ここに宣言します。 システムアドミニストレータの存在は、私たちの日常生活にITが浸透した現代において、ますます重要性を増してきています。その、ITの利用者と提供者の橋渡しとしての役割は、社会のあらゆる舞台で、これからも価値を持ち続けるものと、私たちは確信しています。 私たち日本システムアドミニストレータ連絡会会員は、業務改革を推進し、情報戦略ひいては経営戦略の実現を担う高度IT人材として、社会に貢献し続けることを目指します。そして、あらゆる場面で改革を実現させる強い意志、気概、魂を持って、相互に研鑽しあい、自己のスキルを向上させるとともに、次世代のシステムアドミニストレータを育成していきます。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
3	1	個人	-	ITベンチャーから自動車業界に移り、データエンジニアを行っているものです。 骨子を軽く読みしましたが、データ基盤は基盤自体が中心ではなく、エンドユーザのニーズに合わせて変化して行くべきと考えています。基盤に合わせて最小公倍数的に規則を決めるとエンドユーザの誰にもフィットしない基盤が出来上がるので、一定の範囲である程度自由に動ける枠組みが必要です(今の時期ですとそれがクラウドに該当します)。 実は重要なのは、基盤の規則をトップダウンで決める人よりも、エンドユーザの要件を整理して彼らが使いやすい基盤を整備するコンサルティングの方です。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
4	1	匿名	-	「バリュークリエイション」は「安っすい仕事」だと誤認する。 株式用語でも「バリュー」は「安っすい」「注目されていない」の意味だ。 「メリットクリエイション」にすべき。	いただいた御意見について、"value"は必ずしもそれ単体で「価値が低い」ということを含意するものではなく、単に「価値」を意味する用法が一般的と考えられるため、原案のとおりとさせていただきます。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
5	1	匿名	3-2 ルール間のギャップの分析	3　活用方法 3-2　ルール間のギャップの分析（PP. 17-18） 507行目以降に、「欧州から日本への移転については、移転という「イベント」によって、「場」が欧州のGDPR等の法制度から、日本の個人情報保護法制の下に移る。その際、日本は十分性認定を取得していることから、欧州GDPRで求められているデータ保護が、日本の個人情報保護法制の下でも実質的に確保されていると考えられる。データの「属性」に関しては、データ管理主体に日本拠点が加わるのみであるが、その際、十分性認定により、データ管理主体の変化に関しては事前に認められ、許容されていると言える」との記述がある。 これについては、まずEUの一般データ保護規則（GDPR）という「場」を前提として話をすれば、EU域内から日本国内への個人データの移転で捉えられるべき「イベント」は、「移転（transfer）」のみならず「処理（process）」もあることを忘れてはならない。 つまり、十分性認定はあくまでも「移転」を合法化するための措置であって、EU域内の事業者から日本国内への事業者にデータを提供すること自体については、別途「処理」というイベントに対する合法性（同意や正当な利益等）もなければならない。 これを踏まえれば、後段の「データの「属性」に関しては、データ管理主体に日本拠点が加わるのみであるが、その際、十分性認定により、データ管理主体の変化に関しては事前に認められ、許容されていると言える」という記述は正確ではなく、データの「属性」の変化については、「処理」というイベントとの関係で整理されるべき事項であると考える。	いただいた御意見を踏まえ、596行目以降にて記述を以下のように修正いたします。 ・データの「属性」に関しては、データ管理主体に日本拠点が加わるのみであるが、関連する処理(注釈を挿入)に際して、GDPRの規定する個人データの適法な処理の要件が満たされていることを前提とすると、十分性認定により、データ管理主体の変化に関しては事前に認められ、許容されていると言える。 注釈：ここで、「処理」とは、GDPRにおける定義にならい、「自動的な手段であるか否かに関わらず、個人データ、または個人データの集合に対して行われる、あらゆる単一の作業、または一連の作業」を意味するものとする。
5	2	匿名	3-2 ルール間のギャップの分析	3　活用方法 3-2　ルール間のギャップの分析（PP. 17-18） 513行目以降に、欧州から米国への移転をプライバシーシールドを根拠として行おうとする場合についての記述があるが、まず、2020年の欧州司法裁判所（CJEU）Schrems II事件でプライバシーシールドは無効となっており、現在、米EU間で「強化されたプライバシーシールド」に関する議論が行われているため、無効となったものを前提に議論を進めるべきではないと考える。 その上で、欧州から米国への移転について、「イベント＝移転」という形で捉えているが、プライバシーシールドはいわば部分的十分性認定であり、あくまでも移転を合法化する措置に過ぎない。したがって、EU域内の事業者から米国国内の事業者への個人データの提供という「処理」も「イベント」として捉えられるべきであり、その点が欠落しているように見受けられる。 さらに、515行目以降に、「移転という「イベント」を経て、データ「属性」に関して、データ管理主体の変化の他に、開示範囲に米国政府が加わる形で「属性」が変化していると考えられる」との記述があるが、なぜこの移転単体をもって「開示範囲に米国政府が加わる形で「属性」が変化」しているのかの詳細な論述がなく、あまりにも乱暴な議論のように感じる。 この後の文章においても、「判決文によれば、この「属性」の変化がGDPR上の保護と実質的に同等とは認められないと判断された根拠となっている」との記述があるが、今一度判決文をご一読いただいた上で、本当にこのように判断したのか、ご検討いただきたい。	いただいた御意見を踏まえ、プライバシーシールドに基づく欧米間のデータ移転について述べた600行目以降にて記述を以下のように修正いたします。 ・一方、欧州から米国への移転をGDPR等に定めのある適法な手段に基づいて行おうとする場合、データが米国に所在する状況では、「場」が米国の各種法制度に基づいたものに変化している。 また、603行目以降にて、以下の記述を注記いたします。 ・移転という「イベント」を経てデータの物理的な所在地が米国となることを通じて、データ「属性」に関して、データ管理主体の変化の他に、潜在的な開示範囲に米国政府が加わる形で「属性」が変化していると考えられる。 ・このような状況も反映し、現状では、欧州から米国への個人データの越境移転を、欧州委員会が認めた標準的契約条項（SCC）の締結に基づいて実施することが求められている。そのため、十分性認定に基づきかかる移転を行う日本と米国との間には、欧州からの個人データの越境移転に関するルール間のギャップが存在すると言える。
5	3	匿名	2-2-2 モデル化（「場」）	2-2-2 モデル化（「場」）（PP. 13-14） 「場」の設定は容易ではないと考える。この部分では、各国・地域等の法令、組織の内部規則、組織間の契約等に触れながら、パーソナルデータの保護、知的財産・営業秘密保護、機微技術管理、適切な社会機能の維持の4つのカテゴリが挙げられているが、以下3点を指摘する。 ・各国・地域等の法令の適用範囲は多種多様であり、域外適用をどのように考えるのか、A国所在の事業者Xが、A国からB国のユーザーに越境でサービス提供をしていた場合であって、B国が域外適用規定を有していた場合、A国所在の事業者Xは、A国法令に加えてB国法令にも遵守しなければならない。こうしたケースを踏まえる必要がある。 ・組織の内部規則についても、多国籍企業と純粋国内企業では異なる訳であり、グローバル共通の規則＋特定国向けの規則の組み合わせを有する前者と、単に特定国向けの規則を有する後者とでは異なる訳であり、その点も踏まえる必要がある。 ・4つのカテゴリについても、本当にこの切り分けが適切かつ十分なのかといった点がある他、うまく切り分けられるか重複してしまうかは結局コンテキストや観点次第なのであるから、その点も考慮に入れる必要がある。	いただいた御意見を踏まえ、以下のように記載内容を修正いたします。 ・取り扱うデータの性質や、データを利活用する所在地によっても設定される「場」は変わり得る。その際、現にデータが所在している国の法令のみならず、該当する場合は域外適用規定を有する他国の法令も含めて「場」として特定する必要がある点に留意が必要である。(451行目に追記) ・必要な観点を漏らすリスクを低減しながら検討するためには、例えば下記のような4つのカテゴリから整理することで適切な設定につながると考えられる。(460-461行目にて修正) ・なお、カテゴリの分類はひとつの例であり、フレームワークを適用する対象が位置する文脈や重視する観点等により重複や漏れが生じる場合も想定されることから、必ずしも完全なものではない。(464行目に追記)
6	1	企業	全体	（全体） ＜意見＞ データマネジメントのフレームワークそのものは明快でわかりやすいです。データの連接やトレーサビリティも課題となりますが、このデータマネジメントを誰がどのタイミングでどの領域に対して実施するべきか例示があるとより理解が容易になるのではないかと考えます。 ＜理由＞ 本フレームワークではデータマネジメントのあり方については論じられていますが、誰がデータ流通全体でのデータマネジメントを行うべきかが触れられておりません。 データオーナーはデータの入口・出口の範囲でしか管理することができないため、その外は別のデータオーナーの管轄となります。本書はデータ流通全体でデータマネジメントすべきとされており、誰がすべきか例として示したほうが良いと考えられますため。	データマネジメントを誰がどのタイミングでどの領域に対して実施するべきかという点につきましては、本フレームワークの添付文書(添付A)としてユースケースを作成しておりますので、そちらをご参照いただければと存じます。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
6	2	企業	全体	（全体） ＜意見＞ データマネジメントの履歴そのものをブロックチェーンで管理し、「Proven Data」としてデータそのものを管理する全体機構にトレーサビリティを記録することも方法の一つではないかと考えます。 ＜理由＞ データマネジメントで分析した結果の共有がデータのCIAを担保すると考えられますため。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
6	3	企業	1-1-1 CPSF概論	（P.1-5） ＜意見＞ CPSF概論の冒頭において、データ生成の主体が人以外も含めて生成していることに触れた方が良いのではないかと考えます。 ＜意見＞ フレームワーク骨子全体で触れられている工程の変化（多様なつながりによる非定型的なものへと変化する）に加え、データ自体が人以外に生成されることから、自動生成または自動取得されるデータの真正性の確保が、最初に行うべきデータマネジメントの活動と考えられますため。	いただいた御意見を踏まえ、294行目にて以下のように記載を修正いたします。 バリュークリエイションプロセスにおいて、サイバー空間でやりとりされるデータは、センサーによる計測等の自動的な手段または人手による入力等を介して生成・取得されることによってそのライフサイクルが始まる。
6	4	企業	1-1-1 CPSF概論	＜意見＞ 「経済社会全体のセキュリティ上の課題」とあるが、データに依存しない組織も存在すると思わるため、「経済社会全体おけるデータのセキュリティ上の課題」とするのも一案かと考えます。 ＜理由＞ データに依存しない独立した機構は必ず存在すると考えられますため。	いただいた御意見について、本稿並びに参照先の「サイバー・フィジカル・セキュリティ対策フレームワーク」にて議論している対象は必ずしも「データの」セキュリティには閉じていないと考えられるため、原案のとおりとさせていただきます。
6	5	企業	1-1-2 第3層の位置づけ	（P.1-25） ＜意見＞ 第３層の位置づけについて、モバイルデバイス、5G、クラウドサービス等の普及により経済社会全体が手に入れた、いつでも、どこでも、どんなデバイスからでもデータにアクセスが可能というモバイルファーストの世界観に触れるのも一案かと考えます。 ＜理由＞ 現代においては、従前の限られた場所や時間に応じたデータアクセス環境ではないため、リアルタイムでデータセキュリティライフサイクルマネジメントを実施しなければ、個人および組織のプライバシー、セキュリティ、および身の安全が確保できないことを具体的に記載したほうが良いと考えられますため。	モバイルファーストの世界観において実現される事項については、現状の記載にて包括的に記述していると認識しておりますので、いただいた御意見については、原案のとおりとさせていただきます。
6	6	企業	1-3 本フレームワークの目的	（P.5-137） ＜意見＞ リスクを洗い出す事例としてモバイルアプリによるデータアクセスのセキュリティ確保の必要性について触れるのも一案かと考えます。 ＜理由＞ 組織におけるシステム間のデータ交換に加え、より個人や組織が身近なモバイルアプリからのデータ生成やデータ利用におけるリスク分析についての言及が必要であり、普段の何気ないデータアクセスからプライバシー保護や機微情報へのアクセスに対するフレームワークを意識させる必要があります。データアクセスの中心がIoTという環境の中に、人が主体となるアクセスの大半はモバイルアプリが主体となるアクセスであることは明白と考えられますため。	リスクを洗い出す事例につきましては、本フレームワークの添付文書(添付A)としてユースケースを作成しておりますので、追ってそちらをご参照いただければと存じます。
6	7	企業	2-1-2 リスク分析手順	（P.9-263） ＜意見＞ Step4が完了した後も、３つの要素が変化することでリスクが新たに出現したり変化したりすることが考えられますため、Step4については、「場」「属性」「イベント」が時間の経過とともに変化することを前提にした記述とし、その結果CPSFの利用シーンは、これから開発するシステムを企画する際のリスク分析や、インシデントが発生した際のセキュリティ分析など、と明確にすることも一案かと考えます。 ＜理由＞ 「2-1-2 リスク分析手順」には、Step1からStep3に渡ってデータマネジメントにおけるモデル化を行い、その結果をStep4で適切なセキュリティ対策を講ずることとなっていますが、例えば、CTI(Cyber Threat Intelligence)情報を共有するようなシステムで他の数社と契約締結をして運用をすることを想定すると、企画時に想定される利用目的に合致したリスク分析を完了しても、運用後の新規共有組織の加入や新しい加工法や利用手法の追加、利用するデータセンターの変更などで「場」や「属性」が変化し、それに伴うセキュリティ要件が大きく変わる可能性があるのではないかと推測できます。これは、運用しながら環境や利用法が変わる可能性のあるシステムは、その殆どが最上級の対策の対象となる可能性を示唆しており、システムのライフサイクルにおいてセキュリティ要件が過剰となり得る場合が想定されます。 故に、CPSFの利用シーンは、システム企画の際のリスク分析や、インシデントが発生した際のセキュリティ分析などであると明確にし、特にシステム企画の際のリスク分析の結果については、利用者や利用(加工)方法の制限事項に十分反映させるべきである、などと明確にしたほうが良いと考えられますため。	いただいた御意見も参考に、273行目にて以下の記載を追記いたします。 ・また、STEP 4までの取組が完了した後も、内外の要因により従前に特定した「属性」、「場」、「イベント」の内容が変更されることで、新たなリスクが出現したり、想定していた内容が変化したりすることが想定される。そのため、データ利活用のプロセスやそれを取り巻く環境等に何らかの変更が行われることを認識した場合、STEP 1からSTEP 3までの検討結果をレビューし、改めてリスクポイントの洗い出しを行うことが望ましい。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
6	8	企業	2-2-1 モデル化（「イベント」）	（P.10-286） ＜意見＞ モデル化イベントにおける整理のポイントとして、「生成・取得」「加工・利用」「移転・提供」「保管」「廃棄」に加えて、「アーカイブ」を加えるのも一案と考えます。 ＜理由＞ 組織はリアルタイムでのデータ使用が要求されない場合、法・規制または組織の方針に従い、アーカイブの対応が必要と考えます。その際、アーカイブのデータが組織内またはサプライヤーが再取得した際、アーカイブデータの真正性の確保が必要になります。本フレームワーク内において、利用期限についても言及されていることから、アーカイブのイベントについてもデータセキュリティライフサイクルマネジメントのイベントとして定義する必要があると考えられますため。	データを専用の保存領域や記録装置にて長期的に保存する行為としての「アーカイブ」は、「保管」に含まれるものと考えております。
6	9	企業	2-2-1 モデル化（「イベント」）	（P.12-347） ＜意見＞ システム・サービスにおける、複数の機器（またはサービス）から構成されるデータの移転、提供におけるリスクについて、具体的事例がネットワーク上での盗聴と送信先・送信元のなりすましが示されていますが、アプリケーションや人為的なミスによるリスクを加えることも一案かと考えます。 ＜理由＞ 例えば異なるサービス間で、移転・提供をうけるデータの完全性を担保するにはシステムプログラムの不具合や移送プロトコルの違いによって、データの完全性が失われる可能性は少なくないと考えられますため。	いただいた御意見も参考に、349行目以降にて記述を以下のように修正いたします。 ・これによって、悪意のある者によるネットワーク上での盗聴やデータの移転・提供に係るシステムの不具合等によるデータの損傷等のリスクを捉えることが可能になる。
6	10	企業	2-2-1 モデル化（「イベント」）	（P.12-353） ＜意見＞ 保管については、オンプレミス環境を想定しているように読み取れますが、利活用の進むクラウドサービスプロバイダー等が提供するクラウドストレージの例示を加えることも一案かと考えます。 ＜理由＞ サプライヤー含めた広くデータ共有を促すフレームワークを目指すならば、オンプレミス環境を想定して用語の定義にとどまらず、オフプレミス環境を想定した用語を使う必要が望ましいです。事例については、従前の用語の定義に拘らず、時代に応じた用語を選択すべきと考えます。103から113の記載内において、クラウドサービスに言及していることもあり、重要な例示になると考えらますたため。	いただいた御意見も参考に、419行目以降にて記述を以下のように修正いたします。 データはライフサイクルの様々な段階において、外部サービス（クラウドストレージを含む）やネットワーク接続されたストレージ機器、クライアントのハードディスク、USBメモリのような可搬媒体、機器の一時記憶領域等に保管され得る。
6	11	企業	2-2-1 モデル化（「イベント」）	（P.13-361） ＜意見＞ 「廃棄」本フレームワークにおける廃棄は、データセット全体を使用不可能な状態とすることを指す、とありますが保有するデータを廃棄できても、流通過程で複製されたデータ全てを廃棄することは一般的に困難であると考えられるため、現実的に定義された廃棄は困難ではないかと考えます。 ＜理由＞ 本イベントは論理的な廃棄を意味するものと理解しますが、物理メディアの廃棄と混同される恐れがあり、保有データの消去・消滅など明確な定義を行う必要があると考えられますため。	いただいた御意見も参考に、431行目に以下の記述を追記いたします。 ・データは自組織が直接的に管理する媒体だけでなく様々な媒体に複製され得るが、当該データのカテゴリや重要度等を勘案して、組織は当該データに対する権限や複製、配布等の状況について適切に管理する必要がある。元のデータを廃棄する際に、複製先のデータも含めて廃棄する必要がある場合には、関連するステークホルダーと協調しつつ、廃棄の取組を推進する必要がある。なお、個人の同意に基づいて収集したパーソナルデータに関して、特定の個人が同意を撤回する等により、当該個人のデータをデータセットから除外する行為は、加工・利用の一形態として捉えるのが適切である。
6	12	企業	2-2-3 モデル化（「属性」）	（P.14-408） ＜意見＞ モデル化属性における整理のポイント、447から453の記載内容を、417の先頭に記載することで、整理のポイントのプロセスの流れが理解しやすくなるのではないかと考えます。 ＜理由＞ 447から453に記載がある、価値（重要度）、いわゆる情報資産価値が決まらなければ、組織はどのような取り扱いを行えばよいか方針を決めることが困難であり、そのため、組織が最初に取り組む活動として、価値（重要度）を最初に明示し、他のポイントを記載することが必要であると考えられますため。	ご指摘いただいている通り、データの価値(重要度)はより具体的なデータの取扱いを検討するにあたり優先的な属性と考えておりますが、カテゴリ等の他の属性から見て必ずしも対応の前後関係が認められるものではないと考えられます。例えば、カテゴリ等の他の属性におけるパラメータを特定する中でデータの価値(重要度)を検討するうえで重要なインプットが得られる場合もあると想定されることから、いただいた御意見については原案のとおりとさせていただきます。
6	13	企業	3-2 ルール間のギャップの分析	（P.17-503） ＜意見＞ 「移転」は国家間のデータの移動を指すものと考えられますが、例えばクラウドインスタンスのデータサーバ間の移動は国家間に含まれるか、または、同じ国のクラウドを利用しているが別の国の法人にまたがるものを指すか、などを明確にしたほうが理解は容易になるのではないかと考えます。 ＜理由＞ 論理的な所有権を有する主体の所属する国と、データ・情報が電磁的記録として格納された国が存在すると考えられますため。	352行目以降において、「移転・提供」には国家間のデータの移動だけでなく、組織・ヒト間、システム・サービス間、機器間等、様々な者が含まれる点を改めて追記しておりますので、いただいた御意見については、原案のとおりとさせていただきます。
7	1	個人		自分の理解力のなさはさておき、全般的にわかりにくい文章となっています。もっとわかりやすい表現にしていただくか、一般人にも理解しやすい概要資料を付けていただけると助かります。	ご指摘いただいているような関心に基づき、フレームワークの添付文書としてユースケースを策定する等の試みを進めておりますが、フレークワークのよりわかりやすい発信を含め、更なる検討を進めていくに当たっていただいた御意見を参考にさせていただきます。
8	1	企業	2-1-1 データマネジメントのモデル化の概要	"P7　200" データに対して特定の規範を共有する範囲である「場」について 「場」という表現が、わかりづらいと思います。データに対して特定の規範を共有する範囲である「場」であるより、データに対して考慮しないといけない、規制、ルール、ガイドライン等であると理解するために「規範」といったような表現でよいのではないでしょうか。（規範の中に影響範囲も含まれる）	「場」という概念は、明文化されていないルール等の必ずしも「規範」として扱われない内容を含み得るより広義の概念と理解しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
8	2	企業	2-2-1 モデル化（「イベント」）	"P10　298"「データの生成に関わる機器・システムなどの信頼性」について 今後、スマート保安のように、石油・化学や電力・ガス等の産業・エネルギー、エレベータ・ビルなどの関連インフラで、インフラ関連設備の機器のセンサーから出るデータの活用を使ったサービス（保守・メンテ、診断、監視等）が増えてくることが考えられるため、機器からでるデータの信頼性の基準（何をもって信頼性があると言えるのか）など政府で議論、基準などのガイドラインを示していただきたい。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
8	3	企業	2-2-1 モデル化（「イベント」）	"P11　309"「利用」の定義について 「利用」という表現について、データを第三者に渡す場合も「利用」と言えることから、本フレームワークでいう「利用」（データを利用し やすくした上で、そのデータを閲覧したり、そのようなデータからAI等を利用することでイ ンテリジェンスを抽出することによって付加価値につながる。）は、「分析」の方が、適切に表現できているのではないでしょうか。 「利用」だと、第三者提供と混同するとおもわれるため、混同しないいい回しが必要と考えます。	ご指摘いただいているデータの第三者提供につきましては、通し番号27に対する考え方でも記載した通り、「移転・提供」に該当すると整理しております。また、「分析」という表現を用いた場合に、現在「加工・利用」として整理している一部の内容が認識から漏れてしまうことも想定され得ることから、いただいた御意見については、原案のとおりとさせていただきます。
8	4	企業	2-2-1 モデル化（「イベント」）	"P12　343"　４つの単位について 「そこで、本フレームワークにおいては、ある特定の移転・提供事象について、国・地域、組織・ヒト、システム・サービス、機器という4つの単位で整理することとする。」とありますが、４つの単位について、言葉の定義、説明を追記していただきたい。例えば、システム・サービス とは、サービスを提供するシステムのことか？システムとサービスは常に一緒に扱うのか？など。	いただいた御意見も参考に、352行目以降において移転・提供に係る４つの単位に関する説明を追記いたします。
8	5	企業	2-2-1 モデル化（「イベント」）	"P12　347"　４つの単位で整理したリスクについて 「機器という4つの単位で整理することとする。これにより、技術的・非技術的なリスクを網羅的に識別するにあたり有用と考えられる。それぞれの考慮すべき事象やリスクは下記のとおり整理できる。」とありますが、ここで４つの単位で整理したリスクは、最終的にSTEP１？４を踏まえて得られるリスクとの関係はどのように扱われるのでしょうか。	４つの単位で整理したリスクは、最終的に、STEP4にて洗い出されるリスクに包括されると認識しております。
8	6	企業	2-2-1 モデル化（「イベント」）	"P12　348" イベントをどの程度詳細に記述するかについて 「イベントをどの程度詳細に記述するかは、データフローの整理の目的に応じて調整する必要。」とありますが、例示を示して頂けると整理、理解がしやすいので例示を示していただきたい。	いただいた御意見を参考に、添付文書としてユースケースを作成するにあたり、イベントの記述粒度に関する内容も含めた形で検討をいたします。
8	7	企業	2-2-3 モデル化（「属性」）	"P14　409" 属性について 代表的な「属性」やパラメータ、「属性」の整理のポイントを例示していただいていますが、異なるステークホルダーでこのフレームワークを活用する際には、留意すべき必須のパラーメータがあるべきと考えるので、そこも提示していただきたい。（提示されているパラメーターには必ず含むべきもの、そうでないもの粒度があるのではないか）	適用分野やより具体的な適用シーンごとに属性項目やパラメータの重要度が変動し得ることを考慮すると、必ず含むべきものを提示することには一定の困難があることが想定されると考えております。そのため、いただいた御意見については原案のとおりとさせていただきます。
8	8	企業	2-2-3 モデル化（「属性」）	"P15　440" データ権利者について 個人情報保護の例は提示していただいていますが、産業データに関しても例示していただけると分かりやすいと思います。	いただいた御意見も参考に、519行目以降の記述を以下のように修正いたします。 データ権利者（例：個人情報ならばデータ主体となる本人、事業上有用なデータならば権利元の組織）は当該主体の管理下にあるデータに対して引き続き権利を有すると考えられる。例えば、個人情報保護法上の同意の取り下げや、著作権法等のライセンスに関する規定上の取扱、企業の競争力に関わるデータ(例：製品の設計データ、製造拠点における機器・設備の稼働状況)を提供している場合等は、管理主体が転々と移っていく過程でも、「属性」として管理する必要がある。
8	9	企業	-	全体 ガイドラインのユースケースに応じた使い方の例示 このフレームワークがガイドラインとして発行されると、異なるステークホルダーでの共通理解で使われるべきであると考えます。そのさいに、場面に応じた使い方の例示を示していただきたい。	場面に応じた使い方の例示という点につきましては、本フレームワークの添付文書(添付A)としてユースケースを作成しておりますので、そちらをご参照いただければと存じます。その他の点につきましても、いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
9	1	団体	-	「付加価値を創造しているのは物理特性に依存しないデータである」という文章は、やや誤解を招く恐れがあり、かなり大胆な主張であると考えています。データは現実の物理的な世界からの事実を表すべきであるため、この文章を「データの適切な処理が付加価値を生む」と言い換えることを検討しています。	英語版の原案において、元の表現が、意図した内容に対してやや誤解を招く表現となっていたことから、いただいた御意見も参考に、指摘箇所を以下のように修正いたします。 Data, which is originally independent of physical characteristics, creates added value
9	2	団体	-	「付加価値の創出（バリュークリエイション）の基礎となるデータが、バリュークリエイションプロセスの信頼性を確保するための信頼性の基点でなければならない。」という文章について、なぜデータそのものが信頼性のアンカーポイントとなるのか疑問です。価値創造プロセスの信頼性を確保するためには、信頼できるデータが不可欠であることには同意するが、データの正しさや正確さを確保するための方策が、価値創造プロセスの信頼性を確保するためのアンカーポイントとなるべきである。これにより、次項にも沿ったものとなる。	ご指摘いただいている「データの正しさや正確さを確保するための対策」ではなく、対策の実施有無を問わず、正しい内容を示すデータが信頼性の基点となると捉えているため、いただいた御意見については、原案のとおりとさせていただきます。
9	3	団体	-	「データのライフサイクルには様々な主体が関与し、関与した主体による不適切な措置によって誤ったデータが流通し活用されることになれば、そのデータが関わったバリュークリエイションもまた価値をもたらすことはなく、有害な結果をもたらすことにもつながりかねない」という文章について、「（中略）そのデータを用いた価値創造は、（信頼できる方法で）価値をもたらすことができず、実際に有害な結果を招く可能性がある」という説明を加えたいと考えています。	誤ったデータの活用は、信頼できる方法でも、信頼できない方法でも価値をもたらすことはないと考えられることから、いただいた御意見については、原案のとおりとさせていただきます。
9	4	団体	-	「ここで示されているデータ管理の概念を共有し、このフレームワークを共通の理解を得るための共通のツールとして使用することで、異なるデータ管理ルール等の間で、データがルールを越えて分散していても、同じレベルのデータセキュリティを確保するために、必要な調整を行うことができる」について、本フレームワークは「異なるデータ管理ルール等の間で、データがルールを越えて分散していても、同じレベルのデータセキュリティを確保する」ことに貢献できることに同意します。	本フレームワークに対する肯定的な御意見として承ります。
9	5	団体	-	「その中の第3層の位置づけは既に述べたとおりだが、データ自体に信頼性の基点を置いて包括的なセキュリティ対策を実施するためには、データのライフサイクル全体にわたってリスクを洗い出し、セキュリティ確保のための様々な措置を実施することが必要となる」という文章について、「anchor point of」(基点)を削除することを提案します。	いただいた御意見及び、本稿が参照している「サイバー・フィジカル・セキュリティ対策フレームワーク Version 1.0」における用語定義との関係を考慮し、英語版において「anchor point of」を「basis of」に変更いたします。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
9	6	団体	-	「フィジカル空間からサイバー空間に転写されたデータは第2層の転写機能の信頼性を確保することによってデータの信頼性が確保されるが、サイバー空間では様々なデータが生成・編集・加工され、自由に流通し、かつ、こうした過程はマネジメントの信頼性が確認された企業（組織）によってのみ扱われるわけではない」について、「（中略）そして（原則として）第2階層以外のサイバースペースでも自由に交換されている」を追加することを提案します。	いただいた御意見につきまして、引用元の「サイバー・フィジカル・セキュリティ対策フレームワーク Version 1.0」(CPSF)における記載を尊重し、指定の修正は見送らせていただきます。 他方、参照元であるCPSF及び本稿において、日本語版と英語版の間で必ずしも表現や意味が整合していない箇所が見受けられましたので、指摘箇所(英語版のみ)を以下のように修正いたします。 In the process that various data is created, edited, processed, and freely exchanged in cyberspace, it should be noted data is not handled only by companies (organizations) whose management has been confirmed as trustworthy.
9	7	団体	-	「データマネジメントについて確立した定義は存在しない」という場合、「（セキュリティに関連する）データマネジメントのための確立された定義がない」を追加することを提案する。	指摘箇所以前の文脈では、「データを軸として、データの生成・取得から廃棄に至るライフサイクル全体を視野に入れた対応」に焦点を当てて「データマネジメント」の定義を行っており、必ずしもセキュリティ関連という限定をなさず定義を示していることから、いただいた御意見については、原案のとおりとさせていただきます。
9	8	団体	-	「①の視点から導かれることは、データマネジメントという言葉に対する各人の理解は始めから一致しているわけではないということである」と言う場合、「最初」とは具体的にどの時点を指すのかを明確にすることをお勧めします。	いただいた御意見も参考に、82行目の記述を以下のように修正いたします。 ①の視点から導かれることは、データマネジメントという言葉に対する各人の理解は現時点では一致しているわけではないということである
9	9	団体	-	「ここで示すデータマネジメントの考え方を改めて共有することにより、これまで各組織や各国においてデータ管理に関する議論がなかなか噛み合わず、それぞれが整備したデータ管理に関するルール等の間の調整を図ることが難しかったところ、共通の尺度として本フレームワークを活用してデータマネジメントに関する共通の理解を得ることで、異なるデータ管理のルール等の間について、ルール間を跨いでデータが流通した場合でもデータのセキュリティが同じように確保されるために必要な調整を図ることが可能となる。」とする際には、「ルール」ではなく「ポリシー」という言葉を使うことを提案します。	英語版の文書におきまして、いただいた御意見のとおり、修正いたします。
9	10	団体	-	「本フレームワークは、(中略) データを軸に置き、データのライフサイクルを通じて、データの置かれている状態を可視化してデータに対するリスクを洗い出し」という考えに同意します。	本フレームワークに対する肯定的な御意見として承ります。
9	11	団体	-	これは、データマネジメントをモデル化するための記述スタイル（整理の仕方）を決めようという提案だと理解しました。データの整理方法を決めようとすることで、様々な関係者が情報を共有し、議論が活発になるのは良いことだと考えています。いろいろなモデルがありますが、まずは提案されている「プロパティ」「ドメイン」「イベント」という概念で、使いながらブラッシュアップしていくのが良いと考えています。	本フレームワークに対する肯定的な御意見として承ります。
9	12	団体	-	データレベルでのリスク分析は事例が少ないため、導入が難しいと感じる読者も多いと思います。特に、第2層、第3層にまたがるユースケースが多い製造業でのリスク分析の事例をもっと公開してほしいと思います。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
9	13	団体	-	個人情報やパーソナルデータの取り扱いモデルに重点が置かれている印象を受けました。技術研究開発や製造業における設計書などの知的財産や、生産活動に伴って発生するセンシティブなデータの取り扱いにも焦点が当てられていればなお良いと思います。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
9	14	団体	-	生成・取得に関する記述において、「センサーによるデータの取得など、フィジカル空間の情報が大量にサイバー空間に転写され、リアルタイムに共有されるようになると、サイバー空間のつながりにおけるデータの信頼性を検討する場合、センサー等によって物理的な情報がデータとして正しく転写されているかなど、従来はデータを管理する範疇に捉えられていなかった、データの生成に関わる機器・システムなどの信頼性についても検討する必要がある点に留意が必要である」と述べています。 第2層と第3層が組み合わされ、第2層のデータが第3層に配信される場合、第2層のセンサーデバイスがRoot of Trustとなり、第2層から第3層に配信される過程で信頼の連鎖が形成されることになります。このフレームワークでは提案されているように感じますが、もっとわかりやすい例であれば、データ管理におけるセキュリティのイメージが伝わるのではないでしょうか。	いただいた御意見も参考に、305行目に以下の記述を追記いたします。 例えば、第2層においてサイバー空間への転写が正しく行われるよう、セキュリティ侵害（例：ソフトウェアの改ざん）を受けていない信頼できるIoT機器によりデータを生成し、なりすましやネットワーク上での改ざん等がないようサーバ等へ正確に当該データを送信することを通じて、第3層において利活用するデータの信頼性をデータライフサイクルの初期段階から確保することが可能である。
9	15	団体	-	本資料に記載されているように、ドメインには、国内法の違いや国ごとの法律の違いなど、さまざまなギャップがあります。 このフレームワークの利用者だけでは、調査や方針の決定ができないため、Mは今後もドメインの設定方法について世界に向けて情報発信していきたいと考えています。	本フレームワークに対する肯定的な御意見として承ります。
9	16	団体	-	2章で示したような方法で整理されたモデルが、誰に、いつ、どこで、どのように使われるのか、より具体的なイメージを持つことが望ましいと考えています。 このフレームワークのユーザーがユースケースを持ち寄って課題を抽出することを前提に、その先の活用方法のヒントがさらにあると良いと思います。	ご指摘いただいているような関心に基づき、本フレームワークの添付文書(添付A)としてユースケースを作成しておりますので、追ってそちらをご参照いただければと存じます。
9	17	団体	-	2.2.と同様に、個人情報以外のデータに関する情報も必要だと考えています。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
9	18	団体	-	2.2のように、技術研究開発や製造業での使用例が増えることを期待しています。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
9	19	団体	-	個人データの管理に関する一般的なご意見です。 日本、欧州、米国などの大きな経済圏では、例えばEUのGDPRのように、サイバーセキュリティやプライバシーに関する独自の基準や規制を定めています。本論文では、異なる経済圏でのデータ管理や、関連する政策措置についての記述が追加されると良いと感じています。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
10	1	企業	1.2. データの信頼性確保：データマネジメントの考え方の確立	1. 新たなデータマネジメントの在り方 1.2. データの信頼性確保：データマネジメントの考え方の確立 「異なるデータ管理のルール」を「跨いでデータが流通した場合」のセキュリティ確保に必要な調整を図るため、「本フレームワークを活用してデータマネジメントに関する共通理解を得」たいという考え方に賛同します。	本フレームワークに対する肯定的な御意見として承ります。
10	2	企業	1.3. 本フレームワークの目的	1.3. 本フレームワークの目的 「データのライフサイクルを通じて、データの置かれている状態を可視化してデータに対するリスクを洗い出し、そのセキュリティを確保するために必要な措置」の実現を可能にするという目的に賛同します。	本フレームワークに対する肯定的な御意見として承ります。
10	3	企業	2. 本フレームワークにおけるデータマネジメントのモデル	2. 本フレームワークにおけるデータマネジメントのモデル 2.1. 概要データマネジメントをモデル化するための記述スタイル（整理の仕方）を決めるという提案と理解しました。整理の仕方を決め、種々のステークホルダが情報を出し合い、議論を活性化しようとする取り組みは良い事と考えます。モデルはいろいろあると思いますが、まずは提案された「属性」「場」「イベント」という考え方でスタートし、使う中でブラッシュアップしていくので良いのではないでしょうか。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
10	4	企業	2.1.2.リスク分析手順	2.1.2.リスク分析手順 多くの読者は、データレベルのリスク分析の実施実績は少なく、取組み難いと考えます。特に第2層及び第3層にまたがるユースケースが多い、技術研究・開発および製造業におけるリスク分析の実施事例の充実と公開を期待します。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
10	5	企業	2.2.詳細編	2.2.詳細編 個人情報、パーソナルデータの取り扱いモデルが中心になっている印象を受けます。製造業における設計図書などの知的財産や、生産活動に伴って発生する機微なデータなどの取り扱いがクローズアップされているとさらに良いと考えます。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
10	6	企業	2.2.1.モデル化（「イベント」）	2.2.1.モデル化（「イベント」） 第2層と第3層が組み合わされ、第3層にて第2層のデータが転々流通していく場合、第2層のセンサ・デバイスが信頼の基点(Root of Trust)となり、転々流通していく過程で信頼の鎖(chain of trust)が形成されるケースが考えられます。本フレームワークでも示唆されていると感じますが、より明確に例示として記載するとデータマネジメントにおけるセキュリティのイメージが伝わると考えます。	いただいた御意見も参考に、305行目に以下の記述を追記いたします。 例えば、第2層においてサイバー空間への転写が正しく行われるよう、セキュリティ侵害（例：ソフトウェアの改ざん）を受けていない信頼できるIoT機器によりデータを生成し、なりすましやネットワーク上での改ざん等がないようサーバ等へ正確に当該データを送信することを通じて、第3層において利活用するデータの信頼性をデータライフサイクルの初期段階から確保することが可能である。
10	7	企業	2.2.2. モデル化（「場」）	2.2.2. モデル化（「場」） 場(domains)は、本書に記載の通り国内法の差異、国ごとの法律の差異など、様々なギャップが存在します。 本フレームワークの利用者だけで調査、方針を決められる性質ではないため、引続き場(domains)の設定方法について、世界へ情報発信を期待いたします。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
10	8	企業	3.1. サプライチェーンを構成するステークホルダー間での活用	3. 活用方法 3.1. サプライチェーンを構成するステークホルダー間での活用 2章で示されている方法で整理したモデルを、誰が、いつ、どこで、どのように使うのか、その活用方法について、もう少し具体的なイメージがあると望ましいと考えます。 本フレームワークの利用者が、ユースケースを持ち寄って課題を洗い出したとして、その先の活用方法について、さらなるヒントがあると良いと考えます。	ご指摘いただいているような関心に基づき、本フレームワークの添付文書(添付A)としてユースケースを作成しておりますので、追ってそちらをご参照いただければと存じます。
10	9	企業	3.2. ルール間のギャップの分析	3.2. ルール間のギャップの分析 2-2 と同様に、個人情報以外のデータについても情報が必要と思料します。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
10	10	企業	添付A. ユースケース	添付A. ユースケース 2-2 と同様に、技術研究・開発および製造業におけるユースケースの充実を期待します。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
10	11	企業	添付B. イベントごとのリスクの洗い出しのイメージ	添付B. イベントごとのリスクの洗い出しのイメージ 2-2 と同様に、技術研究・開発および製造業におけるユースケースの充実を期待します。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
11	1	個人		(意見を要約) 提示されている内容については概念的な内容が多く、やや冗長なことから、実用性に懸念がある。 存在する種々のセキュリティ懸案事項への対応を行い、また事業者としてCSO（最高セキュリティ責任者）・CISO（最高情報セキュリティ責任者）等を定めてポリシーを策定する等し、それらを行いつつ、認証を取得しようとする際にはそれに適合・対応した形に幾分か変更を行う、という形がより望ましいのではないかと考える。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
11	2	個人		(意見を要約) なお、国民としては、国がISO認証についての、認証事業者の公表及びその認証を行った機関の提示を行う事を支援していただきたいと考える。（これは本文書にも適合した国という監督的な役割も持つ主体が行うものとして望ましいものであるはずであるが、まず範を示し、事業者間のつながりについて、世間一般的に価値のあるものである事を示されたい。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。