DX企業のプライバシーガバナンスガイドブックver1.0（案）　パブリックコメントに対するご意見とご回答

ID	箇所	御意見の概要	回答
1	ガイドブック全般	ある程度の情報セキュリティの基となるISO27001の概念が入っていない。個人情報保護法の概念は入っているが、ISO27001の概念を含めなければ個人情報の意味をなさないと感じる。もっともJISQ15001:2017「個人情報保護マネジメントシステム－要求事項でA.3.4.3.2の管理策を求め付属書Cは実質ISO27001である。ただ、Pマークを取得する事業者でこの部分に取り組んでいる事業者がどれだけいるだろうか？DXは様々なモノをデータ化する。紙媒体の脱却としては幅広く推進しうるものではあるが、データーをごっそり盗まれる危険性は大いに存在しうる。企業の対策で自己責任でも良いが、監督官庁としては、この部分にもっと注力もして欲しい。利便性とセキュリティは相反する。面倒だ。で、終わらせる事無く推進させて欲しいと願う。	本ガイドブックは、企業がプライバシーガバナンスへ取り組むことの重要性について主に記載しており、プライバシーに係るリスクマネジメントについては、参考として紹介しております。 御指摘の点につきましては、今後の参考とさせていただきます。
2	ガイドブック全般	「サイバーセキュリティー対策」が重要な構造と、私し個人は思います。例えばですが、「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と、私は考えます。具体的には、「電波規格（エレクトロリカルウェーブスペック）」及び「通信規格（トランスミッションスペック）」での「回線（サーキット）」の事例が有ります。（ア）「通信衛星回線（サテライトシステム）」における「トランスポンダー（中継器）」から成る「ファンクションコード（チャンネルコード及びソースコード）」のポート通信での「DFS（ダイナミックフレカンシーセレクション）」の構造。（イ）「電話回線（テレコミュニケーション）」における基地局制御サーバーから成る「SIP サーバー（セッションイニテーションプロトコル）」の構造。（ウ）「インターネット回線（ブロードバンド）」におけるISPサーバーから成る「DNSサーバー（ドメインネイムシステム）」の構造。（エ）「テレビ回線（ブロードキャスト）」における「通信衛星回線、電話回線、インターネット回線」の構造。具体的には、「方式（システムスペック）」での「回線（サーキット）」の事例が有ります。（ア）「3G（第3世代）」における「GPS（グローバルポジショニングシステム）」から成る「3GPP方式（GSM方式及びW-CDMA方式）」の構造。（イ）「4G（第4世代）」における「LTE方式（ロングタームエボリューション）」から成る「Wi-Fi（ワイアーレスローカルエリアネットワーキング）」の構造。（ウ）「5G（第5世代）」での「NR（New Radio）」における「MCA方式（マルチチャンネルアクセス）」から成る「DFS（ダイナミックフレカンシーセレクション）」の構造。具体的には、「情報技術（IT）」及び「人工知能（AI）」での「回線（サーキット）」の事例が有ります。（ア）クラウドコンピューティングでは、「ビッグデータ（BD）」から成る「データーベース（DB）」の導入により、ITネットワークの構造。例えばですが、ファイアーウォールにおける強化では、ルーターとスイッチを挟み込む様に導入する事で、「クラウド側（プロバイダー側）←ルーター⇔ファイアーウォール⇔スイッチ→エッジ側（ユーザー側）」を融合する事で、ハードウェアーの強化の構造。（イ）エッジコンピューティングでは、Web上における「URL（ユ ニフォームリソースロケーター）」での「HTML（ハイパーテキストマークアップラングエッジ）」から成る「API（アプリケーションプログラミングインタフェース）」に導入により、「HTTP 通信（ハイパーテキストトランスファープロトコル）」における暗号化によるソフトウェアーでの「HTTPS（HTTP over SSL/TLS）」の融合により、AIネットワークの構造。具体的には、「サイバー空間（情報空間）」及び「フィジカル空間（物理空間）」での「回線（サーキット）」の事例が有ります。（ア）「サイバー空間（情報空間）」では、「SDN/NFV」における「仮想化サーバー（メールサーバー、Web サーバー、FTP サーバー、ファイルサーバー）」から成る「リレーポイント（中継点）」での「VPN（バーチャルプライベートネットワーク）」が主流な構造。（イ）「フィジカル空間（物理空間）」では、「AP（アクセスポイント）」が主流な構造。要約すると、「ボット（機械における自動的に実行する状態）」による「DoS攻撃」及び「DDoS攻撃」でのマルウェアーにおける「C＆Cサーバー（コマンド及びコントロール）」では、「LG-WAN（ローカルガーブメントワイドエリアネットワーク）」を導入した「EC（電子商取引）」の場合では、クラウドコンピューティング及びエッジコンピーティングにおける「NTP（ネットワークタイムプロトコル）」の場合では、「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、私は考えます。	本ガイドブックの御意見ではないと認識しておりますが、御意見は拝聴いたしました。
3	ガイドブック全般	「DX（デジタルトランスフォーメーション）」における構造では、「製品（プロダクト）、人材（ヒューマンリソース）、研究開発（リサーチアンドデボロップメント）」等の「概念（コンセプト）」での定義を明確にする事が望ましい構造と、私し個人は思います。具体的には、製品における事例が有ります。（ア）破壊的イノベーションにおける「垂直統合（ベイティカルインテグレーション）」では、「量子コンピューター（クアンタムコンピューター）、6G（第6世代）、AI（人工知能）、全脳アーキテクチャー（脳科学）、ゲノム編集（遺伝子工学）」等の構造。（イ）持続的イノベーションにおける「水平統合（ホライゾンテルインテグレーション）」では、「スーパーコンピューター（計算科学）、5G（第5世代）、IT（情報技術）、IoT（インターネットオブシングス）、ロボテックス（機械工学）、仮想技術（VR、AR、MR）、仮想通貨（ブロックチェーン）、EC（電子商取引）」等の構造。例えばですが、「RPA（ロボテックスプロセッシングオートメーション）」では、高い付加価値に対し、効率性を挙げる為には、無駄を削ぎ落とす事で、生産性を向上させる事が望ましい構造と、私は考えます。具体的には、人材における事例が有ります。（ア）新卒一括採用における無期雇用での「事務系（クラーク及びビロー）」を主流としたメンバーズ型の構造。（イ）中途採用における有期雇用での「専門系（スペシャリティー）」を主流としたジョブ型の構造。例えばですが、メンバーズ型における事務系を廃止し、ジョブ型における専門系を導入する事が望ましい構造と、私は考えます。具体的には、研究開発における事例が有ります。（ア）「ウォーターフォール（上流工程から下流工程）」では、「企画（上流工程）、設計及び施工（中流工程）、製造技術（下流工程）」から成る「部品調達及び資材調達（トランスポート）」の構造。（イ）「アジャイル（詳細設計）」では、「0ベース設計（0から図面を引く設計）」及び「ベンチマーク設計（他社製品から比較設計）」の構造。例えばですが、「試作（プロットタイプ）」から「量産（プロダクト）」に至る迄は、ウォータフォールにおける研究開発の場合では、約10年を前倒をして行く事が望ましい構造で有り、アジャイルにおける詳細設計の場合では、約3年を前倒をして行く事が望ましい構造で有ると、私は考えます。「軍事学（ミリタリー）」では、「戦略（ストラテジー）、作戦（オペレーション）、戦術（タクテック）」から成る「兵站（ロジステック）」の構造と、私は考えます。要約すると、「目的（ターゲット）」におけるDXに対し、サイバーセキュリティー対策を導入する事は良い構造なのですが、「手段（プロセス）」における「ノウハウ（Know How）」を政策案での提唱して行く事が望ましい構造と、私は考えます。	本ガイドブックの御意見ではないと認識しておりますが、御意見は拝聴いたしました。
4	ガイドブックタイトル・想定読者	◇　ご質問事項１　「ＤＸ企業のプライバシーガバナンスガイドブックｖｅｒ１．０（案）」というタイトル及び対象企業について 　本ガイドブック本文の中において、「本ガイドブックは、とりわけパーソナルデータを利活用して、消費者へ製品・サービスを提供する中で、消費者のプライバシーへの配慮を消費者から直接的に迫られることが想定される企業や、そのような企業と取引をしているベンダー企業等を対象としている。」と記載されており、ガイドブックの対象となる企業を限定している。しかし、「ＤＸ企業のプライバシーガバナンスガイドブックｖｅｒ１．０（案）」というタイトル自体の意味としては、本ガイドブックに記載されている前記の対象の企業より広い範囲の企業を対象としている印象を与えるのではないか。対消費者限定のガイドブックであれば、タイトルに対消費者限定と明記した方が読者にとって、理解しやすく、分かりやすいのではないか。また、「とりわけパーソナルデータを利活用して、消費者へ製品・サービスを提供する中で、消費者のプライバシーへの配慮を消費者から直接的に迫られることが想定される企業や、そのような企業と取引をしているベンダー企業等」は、全て「DX企業」であると言えるのか。ガイドブックの対象とする企業について再検討すべきではないか。	サイバー空間とフィジカル空間が高度に融合された人間中心の社会であるSociety5.0にむけて、企業は、データの利活用によるイノベーションを創出し、サービス・製品の高度化を通じて、経済成長と社会課題の解決を進める中心的な役割を担っています。 本ガイドブックは、とりわけパーソナルデータを利活用して、消費者へ製品・サービスを提供する中で、消費者のプライバシーへの配慮を消費者から直接的に迫られることが想定される企業や、そのような企業と取引をしているベンダー企業等を対象としていますが、個々の具体例については、企業の規模やリソースに応じた適用が認められるものであり、個々の企業の状況に応じて柔軟に利用していただきたいと考えております。 ご指摘を踏まえて、ガイドブックのタイトルを「DX時代における企業のプライバシーガバナンスガイドブック」と修正いたしました。
5	ガイドブックタイトル・想定読者	◇　ご質問事項２　「ＤＸ企業のプライバシーガバナンスガイドブックｖｅｒ１．０（案）」というタイトル及び対象企業について 　「ＤＸ企業のプライバシーガバナンスガイドブックｖｅｒ１．０（案）」というタイトルで「DX企業」と限定しているが、「DX企業」であるか否かにかかわらず、個人のプライバシーが適切に保護されることが重要であり、特に、「DX企業」と限定して記載しなくてもよいのではないか。また、ガイドブックの対象とする企業について再検討すべきではないか。 　本ガイドブックの1ページにおいて、「本ガイドブックは、とりわけパーソナルデータを利活用して、消費者へ製品・サービスを提供する中で、消費者のプライバシーへの配慮を消費者から直接的に迫られることが想定される企業や、そのような企業と取引をしているベンダー企業等を対象としている。」と記載されており、ガイドブックの対象となる企業を限定している。しかし、「ＤＸ企業のプライバシーガバナンスガイドブックｖｅｒ１．０（案）」というタイトル自体から感じられる意味としては、本ガイドブックに1ページ記載の前記の対象の企業より広い範囲の企業を対象としている印象を与えるのではないか。対消費者向け企業限定のガイドブックであれば、タイトルに対消費者向け企業限定であることを明記した方が読者にとって、理解しやすく、分かりやすいのではないか。 　また、当ガイドブックの用語の定義集も作成し、タイトルにも明記のある、「DX企業」の定義も明瞭に記載した方がよいのではないか。「とりわけパーソナルデータを利活用して、消費者へ製品・サービスを提供する中で、消費者のプライバシーへの配慮を消費者から直接的に迫られることが想定される企業や、そのような企業と取引をしているベンダー企業等」は、全て「DX企業」であると言えるのか。また、「DX企業」は、全て「とりわけパーソナルデータを利活用して、消費者へ製品・サービスを提供する中で、消費者のプライバシーへの配慮を消費者から直接的に迫られることが想定される企業や、そのような企業と取引をしているベンダー企業等」という対消費者に限定した企業のみであるのか。ガイドブックのタイトルと対象とする企業について、そもそもの概念、記載内容等を再検討した方がよいのではないか。	サイバー空間とフィジカル空間が高度に融合された人間中心の社会であるSociety5.0にむけて、企業は、データの利活用によるイノベーションを創出し、サービス・製品の高度化を通じて、経済成長と社会課題の解決を進める中心的な役割を担っています。 本ガイドブックは、とりわけパーソナルデータを利活用して、消費者へ製品・サービスを提供する中で、消費者のプライバシーへの配慮を消費者から直接的に迫られることが想定される企業や、そのような企業と取引をしているベンダー企業等を対象としていますが、個々の具体例については、企業の規模やリソースに応じた適用が認められるものであり、個々の企業の状況に応じて柔軟に利用していただきたいと考えております。 ご指摘を踏まえて、ガイドブックのタイトルを「DX時代における企業のプライバシーガバナンスガイドブック」と修正いたしました。
6	ガイドブック全般	◇　ご質問事項３ 　個人情報保護法令等、個人情報保護法令等のガイドライン、職業安定法等の法令等、プライバシーマーク（JIS Q 15001）、ISO/IEC 27001（JIS Q 27001）等の標準規格等の内容とも整合性が十分とれたガイドブックにした方がよいのではないか。また、それらの法令等、ガイドライン、標準規格等と整合性のとれた用語を使用した方がよいのではないか。 　例えば、引用文献１の個人情報保護法の第二条の（６）においては、英訳として次の記載がある。ガイドブックの「パーソナルデータ」と意味合いがずれているのではないか。ガイドブックの1ページの脚注には、「パーソナルデータとは、個人情報保護法の個人情報だけではなく、個人に関連するあらゆる情報を指す。」と記載されている。用語の使用方法、意味等が異なると、皆がすぐに理解しにくく、浸透する際に時間がかかり、混乱するおそれも憂慮されるのではないか。 引用文献１の個人情報保護法の第二条の定義 「６　この法律において「個人データ」とは、個人情報データベース等を構成する個人情報をいう。 (6)　"Personal data" in this Act means personal information constituting a personal information database etc.」 引用文献１ 法務省．（翻訳日：平成28年12月21日）．日本法令外国語訳データベースシステム - [法令本文表示] - 個人情報の保護に関する法律．参照日　令和2年8月7日，参照先 http://www.japaneselawtranslation.go.jp/law/detail/?id=2781&vm=04&re=01&new=1	本ガイドブックは、企業がプライバシーガバナンスへ取り組むことの重要性について主に記載しており、ご意見でいただいた法令や標準規格等が対象とする中でも、プライバシーに係るリスクマネジメントについては参考として紹介しております。言葉の定義につきましては、必要に応じて脚注により言葉の定義を補足しています。 御指摘の点につきましては、今後の参考とさせていただきます。
7	コラム	◇　ご質問事項４　職場での労働者のプライバシーの保護の明記のお願いとそのお伺い 　職場での労働者のプライバシーの保護については、本ガイドブックの11ページの「コラム -新型コロナウイルス感染症対策とパーソナルデータの活用」において少し触れた記載があるが、本論ではないコラムという扱いの記載である。組織で懸命に働く労働者のプライバシーが保護されるよう、労働者のプライバシーの保護を組織内で真正面に取り組まれるよう本論でも十分に記載すべきではないか。各組織が労働者のプライバシーが積極的に保護すべく取り組むことも重要ではないか。「ＤＸ企業のプライバシーガバナンスガイドブックｖｅｒ１．０（案）」としては、労働者のプライバシーもきちんと保護対象として明記し、ガバナンスの方法等について、詳説し、適切に保護されるべきではないか。職場でのカメラ撮影、鞄の中の私物、オンライン会議時の自宅の風景等には、労働者のプライバシーも含まれる可能性がある。労働契約法、労働安全衛生法、労働基準法等の法令等、ガイドライン等に準拠したガイドブックにした方がよいのではないか。また、これらの法令等、ガイドライン等に本ガイドブックが準拠していること、準拠文献、出典等を本ガイドブックの本文で明記した方がよいのではないか。労働者の肖像権、知的財産にも配慮についてもガイドブックで明記した方がよいのではないか。また、従業員に限らず、役職員についても同様に職場でのプライバシーが保護されるよう、ガイドブックで明記した方がよいのではないか。	従業員のプライバシーの重要性は認識しており、「4.5.1. ステークホルダーへの対応」の「（6）従業員等」に記載しております。 その他御指摘の点については、今後の参考とさせていただきます。
8	4.5.1. ステークホルダーやビジネスパートナーへの対応	◇　ご質問事項５　求職者のプライバシーの保護の明記のお願いとそのお伺い 　職業安定法令等にも規定があるが、求職者のプライバシーの保護については、本ガイドブックにおいて明言がないようであるが、求職者のプライバシーも適切に保護されるべきではないか。履歴書、職務経歴書、適性試験、面接での回答、オンライン面接時の自宅の風景等には、求職者のプライバシーも含まれる可能性がある。 　採用選考におけるプライバシーの取り扱いについては、厚生労働省が全国のハローワーク、「公正な採用選考について」というウェブサイト等で次のパンフレットを含む、各種啓発冊子を長年配布している。これらを含む、職業安定法令等の法令等、ガイドライン等に準拠したガイドブックにした方がよいのではないか。また、これらの法令等、ガイドライン等に本ガイドブックが準拠していること、準拠文献、出典等を本ガイドブックの本文で明記した方がよいのではないか。 引用文献２ 厚生労働省．（令和2年）．事業主啓発用パンフレット：公正な採用選考をめざして（令和2年度版）．参照日　令和2年8月7日，参照先 https://www.mhlw.go.jp/www2/topics/topics/saiyo/dl/saiyo-01.pdf	従業員のプライバシーの重要性は認識しており、「4.5.1. ステークホルダーへの対応」の「（6）従業員等」の中で、求職者についても配慮が必要である旨を明記しました。 その他御指摘の点については、今後の参考とさせていただきます。

DX企業のプライバシーガバナンスガイドブックver1.0（案）　パブリックコメントに対するご意見とご回答

ID	箇所	御意見の概要	回答
9	ガイドブック全般	ｐ１～２　「本ガイドブックの位置づけ」について <意見> 本ガイドブックの位置づけを以下との関係で明確化していただきたい。 1）経産省「デジタル経営改革のための評価指標（「DX推進指標」）」（２０１９年７月公表） 2）DX格付（仮称） 3）デジタルガバナンス・コード（検討中） <理由> 本ガイドブックの内容は、プライバシーに関して取り組むべき方針を定めた重要な文書と認識しており、内容にも賛成いたします。 ただ、これだけ充実したハンドブックですが、企業に対する「強制力」という点が弱いように感じます。 すなわち、企業は、通常、鞭（罰則・課徴金・行政指導、機関投資家からの指摘）かアメ（～銘柄への認定、株価向上）が無い限り、取り組みを行うインセンティブが働きません。一担当者レベルで取り組める課題であれば、その一担当者の個人的なインセンティブ次第で何とかなりますが、プライバシーへの取り組みともなりますと、法務・総務・IT・マーケティングを交えていかねければならず、単なる一個人のやる気ではどうしようもない規模の問題となります。 他方翻って、現状を鑑みますと、コロナ過のため、一部の企業を除きますと、業績の悪化があり、経費削減に大きく舵を切っています。そうしますと、本ハンドブックで謳われているプライバシーへの取り組みが長期的な企業価値（貸借対照表上の「資産」）向上には響くのはわかりつつも、損益計算書やキャッシュフロー計算書の観点からはマイナスに響くため、なかなか前に進めるのが難しいという印象を持っております。現在の「本ガイドブックへの位置づけ」のままで本ガイドブックを社内の関係部署や上司に見せても、社内で必要なヒト（各部の人材のアサイン・人材への研修）・カネ（社内体制、システム投資、外部専門家の起用）を配分してもらえるとは考えにくいです。 そこで、本ハンドブックが企業に対して十分な「アメ」になるようにするために、本ハンドブックをDX銘柄の選定やデジタルガバナンス・コードに盛り込むか言及していただくことで、本ガイドブックに「強制力」が付与され、広く活用されるものとなると考えている次第でございます。 コーポレートガバナンスコードをはじめ、コードはソフトローとして機能しているため、デジタルガバナンス・コードに盛り込むことで「アメ」になると思料いたします。	本ガイドブックは、企業がプライバシーガバナンスへ取り組むことの重要性について主に記載しており、プライバシーに係るリスクマネジメントについては、参考として紹介しております。現在、本ガイドブックの内容について、インセンティブを設定した形での普及・啓発については、想定しておりません。 御指摘の点については、今後の参考とさせていただきます。
10	3.2プライバシー保護責任者の任命	ｐ１６の「３．２　プライバシー保護責任者の指名」 <お願い> プライバシー保護責任者の配置・育成の観点に必要なため、プライバシー保護責任者としてどのような要件が必須・推奨されるのかについてガイドブックにご記載賜れますと幸いです。 具体的には以下の点についてご記載賜りたく存じます。 1）　プライバシー保護責任者の独立性 EUの一般データ保護規則では、DPOには独立性が要求されており、日本でいえば、GDPRのみを担当する監査役のような制度のようです。本ガイドブックで言及されておられる、プライバシー保護責任者というのは、DPOや監査役並みの独立性を有するべきものなのでしょうか。日本のDX企業のプライバシー保護責任者として独立性が必須または推奨されるかにつき、ガイドブックにご記載賜れますと幸いです。 2）　情報管理一般の責任者との兼任 営業秘密をはじめとする企業の情報管理（プライバシー保護含む）を担当する責任者を当社は指名しております。それとは別にプライバシー保護の責任者を指名すべきか、現状通り、情報管理全般を担う責任者がプライバシー保護の責任者も担うという建付けにすべきか悩んでおります。日本のDX企業のプライバシー保護責任者について、情報管理全般とは別にプライバシー保護のみを担当する責任者を指名することが必須または推奨されるかにつき、ガイドブックにご記載賜れますと幸いです。 3）　プライバシー保護責任者の資格 プライバシーに関する資格といいますと、弁護士、個人情報保護士、CIPP（International Association of Privacy Professional）などがございます。DX企業のプライバシー保護責任者というからには、プライバシーについての知見が豊富であることが当然必要とはされますが、それを証明するにふさわしいとお考えの資格等につき、ガイドブックにご記載賜れますと幸いです。 4）　取締役候補者のスキルマトリックスへの記載 現在、大手企業では、取締役候補者のスキルマトリックスを作成する動きが活発化しております（http://blog.livedoor.jp/corporateauditor/archives/22650806.html）。DX企業を名乗るからには、役員級にもプライバシーのスキルを持っている者が必要なのではないかと思っておりますが、「法務」「IT」とは別のスキルとして「プライバシー」というスキルを儲けるべきかについても、ガイドブックにご記載賜れますと幸いです。	プライバシー保護責任者は、一般データ保護規則（GDPR）でいうところの、利益相反規定において、強い独立性が担保されている、データ保護オフィサー（DPO: Data Protection Officer）とは必ずしも同じものとは限らず、役員が担うこともありうると脚注24に記載しております。 本ガイドブックは、とりわけパーソナルデータを利活用して、消費者へ製品・サービスを提供する中で、消費者のプライバシーへの配慮を消費者から直接的に迫られることが想定される企業や、そのような企業と取引をしているベンダー企業等を対象としていますが、本ガイドブックの趣旨に照らして、個々の具体例については、企業の規模やリソースに応じた適用が認められるものであり、個々の企業の状況に応じて柔軟に利用していただきたいと考えております。 その他御指摘の点については、今後の参考とさせていただきます。
11	3.3プライバシーへの取組に対するリソース投入	ｐ１７　「３．３　プライバシーへの取組に対するリソースの投入」 【意見】 ヒト・モノ・カネをどれくらいプライバシーへの取組に投入したかをDX格付などの指標として用いることで間接的にリソースへの投入を促進することができると考える。ご検討賜りたく存じます。	御指摘の点については、今後の参考とさせていただきます。
12	3.3プライバシーへの取組に対するリソース投入	ｐ１７　「３．３　プライバシーへの取組に対するリソースの投入」について <意見> 会社の稟議フローの中にプライバシーに関する検討を踏まえたかという項目を加え、プライバシー保護責任者がその稟議を承認しないと稟議が最終的に承認されないというフローをガイドブックにて推奨すべきと考える。 <理由> 企業に対してプライバシー保護を推奨せよといっても、実際のところウェブサイトに「プライバシーを尊重している」といった言葉が躍るだけになりかねない。そこで、日本の企業文化と調和させつつ、Privacy by Design/Privacy by Defaultを実効あらしめる方法として、稟議フローへ「プライバシー保護観点からの確認」という段階を加えることをガイドブックで謳うべきと考える。 通常、企業の稟議フローでは、契約関係であれば法務、金周りであれば経理・財務が承認フローに入っているが、さらにプライバシー保護責任者が承認するという承認フローも組み込むことで確実にプライバシー保護の観点からのチェックがされると思料する次第である。	本ガイドブックは、企業がプライバシーガバナンスへ取り組むことの重要性について主に記載しており、プライバシーに係るリスクマネジメントについては、参考として紹介しております。本ガイドブックの趣旨に照らして、個々の具体例については、企業の規模やリソースに応じた適用が認められるものであり、個々の企業の状況に応じて柔軟に利用していただきたいと考えております。 御指摘の点については、今後の参考とさせていただきます。
13	2.2. プライバシーの考え方	現在国際的な議論が進展している「ビジネスと人権」の文脈では、プライバシー侵害が技術の進展に伴う新たな人権問題として重視されていることにも触れるべきである。 実際、政府が今秋の公表に向けて現在策定作業を進めている『「ビジネスと人権」に関する行動計画 原案』の「2.分野別行動計画 (1)横断的事項 ウ. 新しい技術の発展に伴う人権」においてプライバシーが取り上げられている。 https://www.mofa.go.jp/mofaj/files/100005380.pdf　（P9～10参照） 本ガイドブック「2.2. プライバシーの考え方」に以下の趣旨の文言を追加してはどうか。 <追加文言案> 現在国際的な議論が進展している「ビジネスと人権」の文脈では、プライバシー侵害が技術の進展に伴う新たな人権問題として重視されてきている（ことに関心を払う必要がある）。 また、政府が策定を進めている「ビジネスと人権」に関する行動計画（NAP）についての記述を追加する（脚注でもよい）。	「2.3. 企業のプライバシーガバナンスの重要性」に、プライバシー問題への対応にあたっては、企業は、サイバー空間を介していても、取扱うのは単なるデータではなく、フィジカル空間の生身の個人と直接向き合っているという事実を改めて認識し、個人の基本的な権利を損なうことのないよう、真剣に考えを尽くすことが必要である。企業の社会的責任の観点からも、消費者あるいは個人の基本的な権利を損なうことのないよう 、プライバシー問題の発生を抑止していくための適切な対応が求められると記載しております。 「ビジネスと人権」に関する行動計画について追記させていただきました。その他御指摘の点については、今後の参考とさせていただきます。
14	2.2. プライバシーの考え方	企業が「プライバシー保護」に注力していくにあたり、「プライバシーとは何か？」について、もう少し説明が欲しいです。 ６ページに「自己情報コントロール権」が書かれており、３５ページに「プライバシー問題の例」が載っていますが、「プライバシーとは何か？」について、もう少し定義や解説がないと、分かりにくいです。 もちろん「プライバシーとは何か？」は年々変化していくのかもしれませんが、それであれば「プライバシーとは何か？」の説明を見直していけばいいだけのように思います。	2.2プライバシーの考え方に、個人へのプライバシー侵害から社会的価値に対する悪影響まで、プライバシーに関して生じる悪影響は多様化しており、個人的な感じ方の相違、社会受容性が、コンテキストや時間の経過によって変わり得るなど、プライバシーという概念を固定して考えられない点に、対応の難しさがあることを記載し、そのような性質のものに対してどのようなリスク管理を企業が組織として行っていくべきかを記載しています。 御指摘の点については、今後の参考とさせていただきます。
15	4.1. 体制の構築	5. (参考)プライバシーリスク対応の考え方」の「5.2. プライバシーリスクの特定(プライバシー問題の洗い出し)」において「ISO/IEC31000 リスクマネジメント」および「ISO/IEC29134:2017」（PIAの実施プロセス及びPIA報告書の構成と内容についてのガイドライン）という2つのISO規格に触れているが、「4. プライバシーガバナンスの重要項目」の「4.1. 体制の構築」において「ISO／IEC 27701：2019」を活用した管理体制の構築について触れることも重要ではないか。 ISO／IEC 27701は、新たな個人データ管理体制の国際標準規格として2019年に発行されたもので、GDPRで求められるさまざまな要件についてもすべてカバーできるように管理策が設計されている。	本ガイドブックは、企業がプライバシーガバナンスへ取り組むことの重要性について主に記載しており、プライバシーに係るリスクマネジメントについては、参考として紹介しております。 御指摘の点については、今後の参考とさせていただきます。
16	ガイドブック全般	・該当箇所 全体 ・意見内容 本ガイドブックでは、プライバシー保護は、個人情報保護法で守られるべき範囲の外側も含めての配慮が必要と説明されており、この点については理解できるが、個人情報保護法の中身や精神とリンクさせた説明が（例えば、利用目的、告知、問合せ対応といった観点で）記載されていると、より分かりやすい。 ・理由 個人情報には必ずしも該当しない、パーソナルデータに関する情報の取り扱いが主になるであろう今後のデータ事業において、現行法との関係記載は重要な拠り所になると考えるため。	本ガイドブックは、個人情報保護法等の法令等遵守を当然の前提としながらも、個人の権利利益や社会的価値への影響を考慮したより積極的な取組や説明について、企業に求められる内容を記載しています。 御指摘の点については、今後の参考とさせていただきます。
17	ガイドブック全般	・該当箇所 全体 ・意見内容 本ガイドブックが対象としている事業者の範囲を明確にしてほしい。Business Contact情報等、プライバシー保護の対象から外れる個人情報のみを取扱っている事業者については、個人情報保護法を遵守すればよく、本ガイドブックの対象ではないことを明確にしていただきたい。 ・理由 Business Contact 情報等、プライバシー保護の対象から外れる個人情報のみを取扱っている事業者については、個人情報保護法を遵守すればよいため。	本ガイドブックは、とりわけパーソナルデータを利活用して、消費者へ製品・サービスを提供する中で、消費者のプライバシーへの配慮を消費者から直接的に迫られることが想定される企業や、そのような企業と取引をしているベンダー企業等を対象としていますが、個々の具体例については、企業の規模やリソースに応じた適用が認められるものであり、個々の企業の状況に応じて柔軟に利用していただきたいと考えております。 一見プライバシーとは無縁に思える情報の取扱いにおいても、本人の置かれている立場や状況によっては重大なプライバシー問題となり得ることもあります（例えば、ビジネスコンタクト情報であっても、悪意のある第三者が閲覧しうるような状態（公開設定）であったりする場合など）。本ガイドブックで紹介するPbDの考え方のように、デフォルトでプライバシーが保護されるような取組がなされていれば、問題を事前に防ぐこともできると考えます。 パーソナルデータを取り扱う企業であれば、一見プライバシーに関係がないように思われる場合であっても、ぜひ本ガイドブックを参照していただければと考えます。

DX企業のプライバシーガバナンスガイドブックver1.0（案）　パブリックコメントに対するご意見とご回答

ID	箇所	御意見の概要	回答
18	ガイドブック全般	・該当箇所 全体 ・意見内容 現在ポピュラーになりつつあるデータ事業における以下の観点を、今後のバージョンアップの際に記載していただきたい。 ① AI 機械学習時の留意観点 ② データ売買時の留意観点 ③ 海外事業者との取引での留意観点 ・理由 商談成立前後は、法律（契約）で管理することができるが、案件アプローチ進行過程での現場への理解促進の意味からも上記観点は重要な知見と考えるため。	プライバシーが意味するもの、あるいはプライバシーに関して起こり得る影響は、「2.2プライバシーの考え方」に、個人へのプライバシー侵害から社会的価値に対する悪影響まで、プライバシーに関して生じる悪影響は多様化しており、個人的な感じ方の相違、社会受容性が、コンテキストや時間の経過によって変わり得るなど、プライバシーという概念を固定して考えられない点に、対応の難しさがあることを記載しております。 今後も本ガイドブックは社会の動向を適切に踏まえながら、更新を行っていきます。
19	1.　本ガイドブックの位置づけ 2.　ガイドブックの前提 4.5 その他のステークホルダーとのコミュニケーション	・該当箇所 「1.　本ガイドブックの位置づけ」「2.　ガイドブックの前提」「4.5 その他のステークホルダーとのコミュニケーション」 ・意見内容 DX においては、クラウドベースによるサービスの開発提供やクラウドリソースの戦略的利活用が不可欠である。そこで、クラウド利用におけるプライバシーガバナンスについて言及すべきと考える。よって冒頭総論部分にクラウド利用を推進しリソース配分を適切に図る現代においては、それに合わせたプライバシーガバナンスのアプローチが求められていることを追加すべきと考える。 また案文の「4.5」は、経済産業省が「2025 年の崖」とも指摘している、従来型のシステム開発委託を念頭に置いたと思われる記述であるため、これを改め、クラウドを利用した場合のいわゆる「責任共有モデル」等と言われる責任分担についても言及し、DX とクラウド利用におけるプライバシーガバナンスについて述べるべきと考える。その場合、データ処理基盤を提供するクラウド事業者が、直接プライバシーにかかわるデータを取り扱わない場合において、クラウドを利用する側の企業がクラウドにおけるプライバシー保護について責任を負うことを明示すべきと考える。また、責任分担の一環として、クラウド事業者側は、クラウド利用者がサービス上の情報を保護するための機能や情報を提供することが望ましいこと、クラウド事業者側のセキュリティについて第三者評価を実施するなどして説明責任を果たすこと、等についても言及されると、クラウドにおける責任共有の考え方が更に明確になると考える。 また、こうした修正は、後述の経済産業省のDX レポート及び個人情報保護委員会の方針等にも沿うものと解される。 ・理由 1．経済産業省のもとに置かれたデジタルトランスフォーメーションに向けた研究会の「DX レポート」（平成30 年）などを始めとして、経済産業省のDX 資料には、DX におけるクラウド利活用の推進が明記されており、プライバシーガバナンスにおいてもクラウドを念頭においた言及があるべきと考える。 2．個人情報保護委員会「『個人情報の保護に関する法律についてのガイドライン』及び『個人データの漏えい等の事案が発生した場合等の対応について』に関するQ&A」（平成29年、令和元年更新）のQ5-33 以下にも、特定の条件を満たす場合、クラウドの利用は個人情報保護法第23 条の「提供」に該当せず、その場合には、クラウドサービスを利用する事業者側において、自ら果たすべき安全管理措置の一環として、適切な安全管理措置を講じる必要がある旨説明されている。 3．総務省「IoT・5G セキュリティ総合対策2020」9 ページ等においても、「クラウドサービスのセキュリティは一般的に『責任共有モデル』が採用されており、クラウドサービス提供者と利用者・調達者の共通の認識の下、それぞれの管理権限に応じた責任分担を行うものである。そのため、クラウドサービス提供者と利用者・調達者は、それぞれの役割を適切に果たすことで、クラウドサービスに関するセキュリティリスクを最小化するために、共に協力することが望ましい」とある。 以上より、クラウドにおける「責任共有」の考え方はプライバシーガバナンスにおいても不可欠となっており、「DX 企業のプライバシーガバナンスガイドブック」においても言及されるべきものと考える。	今日、我々が生きる社会は、デジタル技術の発展とサイバー空間の拡張により、急激な構造転換を迎えている。高度に発達したセンサー、カメラをはじめとする情報取得技術や、あらゆるものをネットワークに繋げるIoT（Internet of Things）によって現実世界（フィジカル空間）のヒトや地上にある様々なモノがインターネットにつながり、それらの情報がクラウド等の仮想空間（サイバー空間）で管理できるようになりつつあります。 企業の中には、受託業務のセキュリティ・可用性・処理のインテグリティ・機密保持・プライバシーに関わる内部統制の保証報告書（いわゆるSOC2レポート）を取得することで信頼確保を図るクラウドサービスプロバイダー等のアウトソーシング事業者が増えつつあることについては、本ガイドブックの中でも脚注20で言及しております。 今後も本ガイドブックは社会の動向を適切に踏まえながら、更新を行っていきます。
20	2.2. プライバシーの考え方	・該当箇所 5 ページ 「機械学習は、静的に記述されたルールではなく、既存状況のデータを統計的に処理したモデルを通じて、対象に関する推定や判断をすることから、新規の対象には対処できず」 ・意見内容 人間による推定や判断についても上記と同様なことが言えるのに、AI の機械学習に対しては「新規の対象には対処できない」と言い切る表現に違和感がある。 ・理由 企業の取り組みを支援するガイドブックに馴染まないと思われるため。	以下のように修正しました。 「対処できず」→「対処することは難しく」
21	2.3. 企業のプライバシーガバナンスの重要性 4.1. 体制の構築	・該当箇所 10 ページ図表3、18 ページ図表6 等、全般 ・意見内容 「個人情報保護」と「プライバシー保護」の包含関係を明確に整理・定義していただきたい。個人情報保護の一部はプライバシー保護の領域に包含されていないように図示されていが、包含されない事項があれば具体的に示していただきたい。 ・理由 個人情報保護の一部はプライバシー保護の領域に包含されていないように図示されているが、図表3 においては、個人情報保護とプライバシー保護全体「事業者が配慮すべき範囲」、図表6 においては、個人情報保護とプライバシー保護全体をプライバシー関連としており、企業経営者等にとって、このガイドブックの対象範囲の特定が難しいと思われるため。	図の主旨を、企業が守るべきプライバシー保護の範囲を示すものとして明確にし、表現を見直しました。
22	3.1. プライバシーガバナンスに係る姿勢の明文化	・該当箇所 15 ページ ・意見内容 ガイドブックの15 ページにアカウンタビリティの重要性についてコメントが記載されているが、概要版にもアカウンタビリティの重要性に関してコメントを記載いただきたい。 ・理由 GDPR 第5 条などにもアカウンタビリティが定義されており、グローバルな動きとしてもキーワードになっているため。	御指摘を踏まえて、修正いたしました。
23	3.1. プライバシーガバナンスに係る姿勢の明文化	・該当箇所 15 ページ 3.1. プライバシーガバナンスに係る姿勢の明文化（プライバシーステートメント、行動原則）に関して ・意見内容 脚注20 に、現行よく見られる「プライバシーポリシー」とは異なる旨、記載があり、個人情報保護法との関係が説明されているが、なぜこれでは足りないと示唆されているのかが馴染みにくく、わかりにくい。個人情報保護法の観点に係る「プライバシーポリシー」に加えて、プライバシーステートメントや行動原則をさらに設ける必要性を訴えるにあたっては、それぞれの明文規定の守備範囲（コンプライアンス/アカウンタビリティ）、およびその連動性を示していただき、双方の明文規定を整備しようと考える事業者が参考にできるような規定の体系例を示していただきたい。 ・理由 個人情報保護法の外側にある、プライバシー遵守精神の明文化については議論が成熟しておらず、理解が難しいのが現状であると考えるため。	本ガイドブックでは、経営者がプライバシーガバナンスを経営上の重要事項の1つと認識し、プライバシーガバナンスに係る姿勢を明文化すること記載しております。どのような形で明文化するかについては、定めるものではないことから、脚注23について主旨が明確になるよう、修正しました。 今後も本ガイドブックは社会の動向を適切に踏まえながら、更新を行っていきます。
24	4.1.1. プライバシー保護責任者の役割	・該当箇所 19 ページ5 行目 「プライバシー保護責任者は、経営者が姿勢を明文化した内容等を踏まえて、実践のための方針を確立し、プライバシーリスクを把握、評価し、対応策を検討できる体制を構築して、方針の実施を徹底する。」 ・意見内容 下線部のようにプライバシー保護責任者に明確な権限を付与する旨を追加すべきである。 「プライバシー保護責任者は、経営者が姿勢を明文化した内容等を踏まえて、経営者から委譲された権限に基づき実践のための方針を確立し、プライバシーリスクを把握、評価し、対応策を検討できる体制を構築して、方針の実施を徹底する。」 ・理由 経営者は、複数部署の間に立って調整することも求められるプライバシー保護責任者に対して、責任だけでなく権限も付与しなければ、関連部署の協力が得られない場合に機能しなくなるおそれがあるため。図表９からプライバシー保護責任者は事業部等に指示を出す権限があるように読み取ることもできるが、本文にも記載し明確化を図るべきと考える。	御指摘を踏まえて、修正いたしました。
25	4.4. 消費者とのコミュニケーション	・該当箇所 24 ページ以降全般 ・意見内容 全般的に「消費者」という表現は「個人」や「データ主体」(GDPR 等で使われているdatasubject の邦訳)等のような表現に統一していただきたい。 ・理由 DX の対象となるパーソナルデータは、B2C 事業の受益者としての「消費者」から収集するケースが多いものの、「従業員」やB2B 事業における「法人顧客」のデータ、さらにはパブリックスペースで収集した「大衆」のデータを活用することもあり、一般的な意味での「消費者」に限定されないため。	本ガイドブックでは、パーソナルデータを活用する企業の皆様に広く活用いただくことを想定し、基本的に「消費者」との表現を採用しております。なお、一部権利主体としての意味合いが強い部分につきましては「個人」との表現を用いております。
26	4.4.2. 消費者との継続的なコミュニケーション	・該当箇所 26～27 ページ 消費者とのコミュニケーション ・意見内容 表現がB2C の運用ベースで記載されている。B2B2C の場合での、左端のB の立場（システムベンダー・データ分析企業・ソリューション提供企業等）は、情報オーナーではないため、基本的に直接的な消費者コミュニケーションを取ることが難しいことが想定されるが、その場合であっても例示されている「意識調査」のほかに、そうしたベンダーの立場としての取り得る施策について、具体化していただきたい。例えばベンダーの立場としてのプライバシーステートメントを公表していくことは効果的なのか、あるいはそこまでは不要なのかについて、指針をお示しいただきたい。 ・理由 ソリューション提供者＝情報オーナーではないが、その立場としての消費者コミュニケーションに関する指針が不明確であるため。	御指摘の点につきましては、参考とさせていただき、今後実際のプラクティスなどを踏まえながら、更新を検討していきます。
27	4.4. 消費者とのコミュニケーション	・該当箇所 28 ページ図表13 ・意見内容 図の左側の「消費者」に向かっている矢印の示す「行為」を明記していただきたい。 ・理由 図中、他の矢印に関しては、ステークホルダーに対する行為が記載されているが、上記に関してのみ未記載であるため。	御指摘を踏まえて、修正いたしました。
28	4.5.1. ステークホルダーやビジネスパートナーへの対応	・該当箇所 29 ページ ステークホルダーとのコミュニケーション ・意見内容 表現がP26～27 と同様に、B2C の運用ベースで記載されている。取引先コミュニケーションのシミュレーション例示がより具体的に記載され、かつ取引関係のバリエーションを想定した記載があればより良いと考える。 ・理由 ステークホルダーの位置付けの図がB2C ベースであって、B2B2C のモデルとの差異がある。例示されている事例では、プライバシー保護観点の対応に応える技術や説明の充実については取引先（ベンダー）の責任とされており、発注側企業はそれを要求するにとどまるケースのみが記載されているが、取引形態によっては、どのような技術や説明ツールを備えるべきかを、発注側企業が仕様としてベンダーに指定する一次責任を負うケースもあるのではないかと考えるため。	発注側企業が、プライバシー問題に能動的に適切に対処すべきことは、本ガイドブック全体を通じて記載をしているところです。図表14として示した取引先とのコミュニケーションは、有効な対応の1事例として示しておりますが、発注側企業から取引先（ベンダー）へ技術や説明を（実際にはRFPなどで）要求する際に、具体的な技術や説明ツールについてどこまでの粒度で要求するのかは、ケースによって様々であることから、現時点ではガイドブックに記載をしておりません。 御指摘の点につきましては、参考とさせていただき、今後実際のプラクティスなどを踏まえながら、更新を検討していきます。

ID	箇所	御意見の概要	回答
29	5.1. 関係者と取り扱うパーソナルデータの特定とライフサイクルの整理	・該当箇所 32～33 ページ ・意見内容 「データの再提供」という表現があるが、図表15 を見る限り、単にA 社からB 社にデータを提供するだけであるから、「データの提供」という表現の方が適切である。 ・理由 個人情報保護法における表現に合わせた方が、読者が理解しやすいため。	御指摘を踏まえて、修正いたしました。
30	ガイドブック全般	（１）　標題について 「DX企業の」を削除し、単に「プライバシーガバナンスガイドブック」とすべきである。 本ガイドブックには以下の記述がある。「イノベーションの創出による社会課題の解決とともに、プライバシー保護への要請が高まっている。この要請に対し、企業は、消費者のプライバシーを可能な限り守ること、その姿勢を貫くことにより、消費者からの信頼の獲得につなげることが、企業のビジネスにおける優位性をもたらしうる」（1頁）。まさしく正論であるが、プライバシーを守ることによってステークホルダーの信頼を確保すべきことは、DXをテーマとして掲げる企業のみならず、すべての企業に妥当することである。また、この理は、企業のみならず、研究機関、教育機関、NPO法人等すべての個人情報取扱事業者に妥当することでもある。「DX企業の」という限定を付することにより、これら個人情報取扱事業者に「我々は無関係」という誤解を生じかねないため、この限定は不要であると考える。	ご指摘を踏まえて、ガイドブックのタイトルを「DX時代における企業のプライバシーガバナンスガイドブック」と修正いたしました。 サイバー空間とフィジカル空間が高度に融合された人間中心の社会であるSociety5.0にむけて、企業は、データの利活用によるイノベーションを創出し、サービス・製品の高度化を通じて、経済成長と社会課題の解決を進める中心的な役割を担っていることから、企業を主な対象とした内容としております。 御指摘の点につきましては、今後の参考とさせていただきます。
31	ガイドブック全般 想定読者	（２）　想定読者について 本ガイドブックの想定読者は、「・データ利活用やデータ保護のガバナンスに携わる企業の経営者または経営者へ提案できるポジションにいる管理職等・経営者の直下でデータの利活用や保護に係る事柄を総合的に管理する部門の責任者・担当者」（１頁）とされているが、（１）記載のとおり、本ガイドブックはより広く個人情報取扱事業者全般に読まれるべきものではないか。また、そのこととの関係で、用語については極力平易な説明があることが望ましいと考える。具体的には、「プライバシーインパクト」(1頁、四角の中の下から２行目）、「ライフログ」（11頁四角内）、「透明性レポート（transparency report）」（24頁）などである。	御指摘を踏まえて、修正いたしました。
32	2.2. プライバシーの考え方	（３）　脚注8（6頁） 現在の位置よりも、5頁の19行目の方が適切ではないか。	脚注9は、プライバシーという概念の発展及び技術進展により、プライバシーに関する新しい問題が含まれるようになってきていることを、実際の具体例で補足するために、例示として記載しています。
33	2.2. プライバシーの考え方	（４）　防犯カメラの社会的受容性（6頁15行目） 「今では一定の配慮の下で設置されることに対する社会の受容性は高まっている」と記載されているが、そのように言えるか疑問である。	防犯目的のカメラについては、個人情報保護委員会の「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するQ＆Aに、「防犯目的については、防犯カメラにより、防犯目的のみのために撮影する場合、「取得の状況からみて利用目的が明らか」（法第 18 条第４項第４号）であることから、利用目的の通知・公表は不要と解されますが、防犯カメラが作動中であることを店舗の入口や設置場所等に掲示する等、本人に対して自身の個人情報が取得されていることを認識させるための措置を講ずることが望ましいと考えられます。更に、カメラ画像の取得主体や内容を確認できるよう、問い合わせ先等について店舗の入り口や設置場所に明示するかあるいはこれを掲載した WEB サイトの URL 又は QR コード等を示すことが考えられます」と記載がされております。他方で、防犯目的以外の利用目的の場合については、経済産業省・総務省より「カメラ画像利活用ガイドブックver2.0」が公開されるなど、その利活用についての社会受容性について議論がなされております。 上記の点や御指摘を踏まえて、以下のように修正いたしました。 「高まっている」→「高まりつつある」
34	4.1.1. プライバシー保護責任者の役割	（５）　プライバシー保護責任者の役割（19頁4行目以下） 近時、DXの潮流にともなって、一部の企業にCDO（チーフ・データ・オフィサーまたはチーフ・デジタル・オフィサー）の役職を置く動きが見られる。CDOは、会社全体のデータ利活用を所管する役職であるが、プライバシー保護責任者とCDOがどのような関係に立つかについての記述があることが望ましい。具体的には、まず、プライバシー保護責任者をCDOに兼任させることは妥当ではないと考えられる。なぜならば、プライバシー保護はCDOが配慮すべき事項であるものの、データ利活用を本務とするCDOの機能と相いれない面があるからである。また、プライバシー保護責任者を完全にCDOの監督下に置くことも、データ利活用が全般的にプライバシー保護に優先する結果となりかねず、やはり適切ではないものと思われる。	脚注24を追記し、「プライバシー保護責任者は、一般データ保護規則（GDPR）でいうところの、利益相反規定において、強い独立性が担保されている、データ保護オフィサー（DPO: Data Protection Officer）とは必ずしも同じものとは限らない。DPOは組織内において個人データの取扱いの目的及び方法を決めることにつながる地位（役員等）に就けないとされているが、プライバシー保護責任者は組織内において個人データ処理の目的及び手段の決定に関与する権限のある役職（役員クラス）が担うことで効果的に機能する場合もありうる。企業に特有の組織構造に応じて、適切な立場の者をプライバシー保護責任者として指名することが望ましい。」と記載しました。 本ガイドブックは、CDOに限らず、CIO、CISO、CPO等が兼務することを排除するものではありませんが、個々の具体例については、企業の規模やリソースに応じた適用が認められるものであり、個々の企業の状況に応じて柔軟に利用していただきたいと考えております。 御指摘の点につきましては、今後の参考とさせていただきます。
35	4.1.1. プライバシー保護責任者の役割 4.1.2. プライバシー保護組織の役割	（６）　プライバシー保護責任者の役割およびプライバシー保護組織の役割（19頁） これらについては、その役割について、従来の所管（たとえばコンプライアンス担当役員や法務部）との比較を表にして示すなどした方が分かりやすいと思われる。	本ガイドブックでは、プライバシーガバナンスの概念を浸透させ、取組みへの着手を優先するべきとの考え方から、「4.1.2.プライバシー保護組織の役割」において、プライバシー保護組織は、企業によって設置する形態は異なり、例えば、専門的な知見を有する専任者を確保が困難な場合には、兼務の従業員のみで保護組織を構成するなど、自社のリソースに合わせて実効性のある組織を構築することが大切であるとしております。 プライバシー保護組織の組成の仕方には、情報セキュリティ部門、監査部門、法務部門等の既存の組織を基礎に、プライバシーガバナンスの機能を組込む等考えられます。本ガイドブックでは、多様な在り方を許容しているため、プライバシー保護組織に対して詳細な要件や機能を定めておりません。 御指摘の点につきましては、参考とさせていただき、今後実際のプラクティスなどを踏まえながら、更新を検討していきます。
36	2.3. 企業のプライバシーガバナンスの重要性 4.1. 体制の構築	（７）　図表３および図表６ 本ガイドブックは、「プライバシー問題」が単なるコンプライアンス（法令遵守）の問題ではないことを適切にとらえている。具体的な記述は以下のとおりである。 「これまで企業がビジネスを行う上でプライバシー問題を考える際には、コンプライアンス＝法令等遵守の観点から、『個人情報保護法を遵守しているか否か』が問われ、多くの場合、その点を中心に検討することで事業が行われてきた。一方で、新たなプライバシー問題の発生や人々のプライバシー意識の高まりという状況変化の中で、必ずしも個人情報保護法の遵守の範囲にとどまらない形で、企業がプライバシー問題に関する批判を避けきれず、いわゆる『炎上』する事例が散見されるようになってきた。」（8頁14行以降） 「これに対して、国内外を問わず、顧客や消費者の信頼を得ながらパーソナルデータを利活用した新たなビジネスを拡大させている企業も少なくない。これらの企業においては、プライバシー保護を企業にとって単なる『コンプライアンス』とはみなさず、重要な経営戦略の一環として捉え、自社ビジネスに関連して起こり得るプライバシーリスクを適切に評価して対応する仕組み・体制を構築するよう、経営者が積極的に取組を推進するとともに、ステークホルダーや社会に対して発信し、プライバシーリスク対応を超えた社会的信頼の獲得を追求している」（9頁1行目以降） このように、本ガイドブックにおける「プライバシー問題」は、法令遵守とは別のものと定義されており、その点が本ガイドブックの重要なメッセージとなっている。ところが、標記の図表３および図表６においては、「プライバシー問題」「プライバシー保護」という表現が特に説明なく用いられており、さらにベン図において「個人情報保護法」と対比して記載される結果、図表３および図表６における「プライバシー」が、あたかも不法行為としてのプライバシー侵害のことであるかのような印象が生じている。この点の誤解を避けるため、図表３および図表６における「プライバシー」が法令違反の問題ではなく、社会的受容性の問題であることを明記することが望ましい。	御指摘のように社会受容性の問題もプライバシー問題に含んでいることは、図中の例示で示しているところです。またこのことがより明確になるよう、「2.3.企業のプライバシーガバナンスの重要性」の本文中にも、以下の追記をさせていただきました。 「必ずしも個人情報保護法の遵守の範囲にとどまらない形で、企業に対して社会的受容性の観点から疑問が投げかけられたり、 企業がプライバシー問題に関する批判を避けきれず、いわゆる「炎上」する事例が散見されるようになってきた。」
37	4.1. 体制の構築	（８）　図表７（19頁） プライバシー保護責任者とプライバシー保護組織の間の矢印が、プライバシー保護組織からプライバシー保護責任者への一方向となっている。プライバシー保護組織について「プライバシー保護責任者へ報告し、指示を仰ぐ必要がある」（20頁24行目）との記述からも明らかなとおり、プライバシー保護責任者はプライバシー保護組織に対して指示等をするのであるから、この部分の矢印は双方向的なものであるべきである。 同様に、経営者とプライバシー保護責任者の間の矢印も、経営者からプライバシー保護責任者への一方向となっている。「プライバシー保護責任者は経営者に対し報告を行い、経営者は、その内容が、プライバシーガバナンスに係る姿勢を明文化した内容と合致しているかを確認・徹底する」（19頁10行目）との記述からも明らかなとおり、プライバシー保護責任者は経営者に対して報告を行うのであるから、この部分の矢印も双方向的なものであるべきである。	御指摘を踏まえて、修正いたしました。
38	5.1. 関係者と取り扱うパーソナルデータの特定とライフサイクルの整理	（９）　32頁15行目および図表15 32頁15行目は、「データの取得からデータの再提供や廃棄」となっているが、この「再提供」は、「提供」の誤記ではないか。図表15も同様である。	御指摘を踏まえて、修正いたしました。
39	4.5.1. ステークホルダーやビジネスパートナーへの対応	（１０）　29頁13行目以下 「このため、プライバシー保護の観点からも適切な対応ができる委託先を選ぶべきであり、対応に関わる体制・技術などの説明を委託先に要求すべきであり、同時に委託元のプライバシーへの取り組みを高まるように委託先が協力すべきである。プライバシー問題が起きたときは委託元がその顧客や消費者に対して真摯に対応するべきである。」とあるが、委託先の体制・技術水準は委託先の選定に先立って委託元が把握しておくべきであること、委託先の委託元に対する協力はインシデント発生時のような場面においては認められるが平時において無償・無条件で認められるべきものではないことから、以下のように修文すべきである。 「このため、委託元は、委託先の体制・技術水準を把握したうえで、プライバシー保護の観点からも適切な対応ができる委託先を選ぶべきである。プライバシー問題が起きたときは委託元がその顧客や消費者に対して真摯に対応するべきであり、委託先にプライバシー問題の発生原因がある場合には、委託先も当該対応に協力すべきである。」	ビジネスパートナー（取引先・業務委託先）とのコミュニケーションにおいては、平時においても、ビジネスパートナーを含めてプライバシー問題に適切に対応することが必要です。業務委託先の協力は必要だと考え記載していますが、無償・無条件ですべきであるとは記載しておらず、取引の形態により柔軟な対応をいただくことを想定しております。
40	4.4. 消費者とのコミュニケーション	（１１）　4.4 消費者とのコミュニケーション（24頁15行目以下） 4.4.1において透明性レポートが紹介され、4.4.2においてサービス機能の追加や利用規約の変更について説明されている。消費者とのコミュニケーションについては、従来より、プライバシーポリシーや利用規約を分かりやすく記載する、記載事項の順序を工夫する、といったより基本的で前提とされるべき工夫・取り組みが存在し、すでにこれまで様々な検討がなされてきたところである。本ガイドブックにおいては、新規性のある工夫・取り組みの紹介のみならず、ベストプラクティスの全体像についての説明がある方が望ましいように思われる。	消費者とのコミュニケーションにおいて、説明の分かりやすさも大切な点の1つであることを明確に記載しました。 その他御指摘の点につきましては、今後の参考とさせていただきます。

ID	箇所	御意見の概要	回答
41	4.5.1. ステークホルダーやビジネスパートナーへの対応	（１２）　従業員（30頁31行目以降） 従業員のプライバシーへの配慮については、「企業は従業員のプライバシーに関する情報を取り扱うことが多いことから、従業員へのプライバシー配慮が必要となる」との記述にとどまっている。従業員のプライバシーに関する行き過ぎた監視等HRテックの不適切な利用については、今後「プライバシー問題」として対応が必要となる可能性が極めて高い論点であるから、その旨を追記して、読者の注意を促すことが適当と考える。	（6）従業員等では、HRテックを導入する場合に限らず、企業が従業員のプライバシーに係る情報を取り扱う場合に配慮や十分な説明が重要である旨を記載しています。 今後も本ガイドブックは社会の動向を適切に踏まえながら、更新を行っていきます。
42	ガイドブック全般	◇　ご質問事項６　ISO、JIS等の標準規格の認証制度自体の限界、悪用、欠陥等のおそれについての再検討のお願い及びお伺い ISO/IEC、JIS等の標準規格が本ガイドブックで何種類も紹介されている。しかし、本年、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（案）（経済産業省　商務情報政策局 情報産業課　ソフトウェア・情報サービス戦略室）のパブリックコメントに対しても私はお伝えしたが、標準規格制度自体の限界、悪用、欠陥等も憂慮している。下記に問題の一部を補正し、抜粋したが、詳細は、前記のパブリックコメントを参照されたい。今般のパブリックコメントの「パーソナルデータ」等の適正な運用も同様に標準規格制度の実際の現場での運用の形骸化、「仏作って魂入れず」等の悪影響も憂慮される。また、ISO/IEC、JIS等の標準規格の詳細な文書が有料であるため、全ての人が簡単に全てを直ぐに閲覧できないため、迅速な理解が進まない。 問題１：委託先、その再委託先等がＩＳＭＳ認証、ＰＭＳ認証等を取得しているといっても、委託先、その再委託先等で情報セキュリティ、個人情報の問題を巧妙にもみ消すおそれがあること 問題２：委託先、その再委託先等がＩＳＭＳ認証、ＰＭＳ認証等を取得しているといっても、内部でもみ消していた場合、ＩＳＭＳ認証機関に通報しなければ、情報セキュリティ、個人情報の問題が放置されてしまう場合があること 問題３：委託先、その再委託先等がＩＳＭＳ認証、ＰＭＳ認証等を取得しているといっても、内部でもみ消していた場合、ＩＳＭＳ認証機関が毎年の審査時にも情報セキュリティ、個人情報の情報事故等の問題に何年間も全く気付かない場合があること 問題４：委託先、その再委託先等がＩＳＭＳ認証、ＰＭＳ認証等を取得しているといっても、組織内部の情報セキュリティに関する規程が曖昧である場合（情報セキュリティの喪失、情報セキュリティ事象、情報セキュリティインシデント等の曖昧な定義等）、情報セキュリティ、個人情報等の情報事故の問題をもみ消せること 委託先、その再委託先等がＩＳＭＳ認証、ＰＭＳ認証等を取得しているといっても、外部のＩＳＭＳ認証機関は、審査時にも実際より情報セキュリティ、個人情報の問題が過少申告されていることに全く気が付かない場合もある。ＩＳＭＳの事務局の情報セキュリティに関するインシデント一覧と運用組織の障害管理台帳等のインシデント一覧との二重帳簿、裏帳簿等で悪く運用されている場合がある。故意に都合よくインシデント件数を操作できる場合がある。 補足すると、報告対象の情報セキュリティの問題の定義を曖昧にして、情報事故をもみ消す方法以外にも、システム関連業務の委託先、その再委託先等のＩＳＭＳ認証、ＰＭＳ認証等の適用範囲に医療機関等がそれらの委託先等との間で委託契約した業務範囲が含まれていないので、杜撰に情報が取り扱われるおそれもある。つまり、委託先、その再委託先等がＩＳＭＳ認証、ＰＭＳ認証等を取得しているといっても、ＩＳＭＳ認証、ＰＭＳ認証等の適用範囲外である場合、ＩＳＭＳ認証、ＰＭＳ認証等のとおりに適切に情報が取り扱われるかは、不透明であり、情報事故等をもみ消せるおそれもある。 問題５：情報セキュリティに関する不正を告発した通報者が保護されない場合があること 経験上、現状は、正しいルールを組織内で確認すること、教育活動を実施することすらしにくい。現状は、法規及び社内規程上、情報保護のための正しい行動もしにくい。公益通報者保護法、社内の公益通報者保護規程等で通報者を適切に保護するべきである。現場で情報セキュリティを維持する現場の労働者及び通報者を適切に保護するよう、個人情報保護法、公益通報者保護法等の関連法令等、様々な情報セキュリティに関するガイドラインに明記し、保護していただきたい。 問題６：今般のCOVID-19の場合のような異常事態時の対応のあり方	御意見は拝聴いたしました。
43	ガイドブック全般	１． 該当箇所　タイトル DX 企業のプライバシーガバナンスガイドブック 意見内容 『DX企業の』という文言は不要である 理由 ・『DX企業』の定義があいまいで具体的にどのような企業を指すのか不鮮明 ・本ガイドブックに書いてあることは DX にどの程度力を注ぐかという事業計画に依存せずとも、データを取り扱う企業が取り組むべき汎用性の広い内容であること	サイバー空間とフィジカル空間が高度に融合された人間中心の社会であるSociety5.0にむけて、企業は、データの利活用によるイノベーションを創出し、サービス・製品の高度化を通じて、経済成長と社会課題の解決を進める中心的な役割を担っています。 本ガイドブックは、とりわけパーソナルデータを利活用して、消費者へ製品・サービスを提供する中で、消費者のプライバシーへの配慮を消費者から直接的に迫られることが想定される企業や、そのような企業と取引をしているベンダー企業等を対象としていますが、個々の具体例については、企業の規模やリソースに応じた適用が認められるものであり、個々の企業の状況に応じて柔軟に利用していただきたいと考えております。 ご指摘を踏まえて、ガイドブックのタイトルを「DX時代における企業のプライバシーガバナンスガイドブック」と修正いたしました。
44	ガイドブック全般 想定読者	２． 該当箇所　P１　２１行目 「経営者の直下でデータの利活用や保護に係る事柄を総合的に管理する部門の責任者・担当者」 意見 想定読者は広く対象とすべき 理由 ・プライバシー保護責任者またはその候補者を想定読者として考えていることを暗示するが、「プライバシー保護責任者は経営者の『直下』のものでなければならない」という定めはどこにもない	ご指摘を踏まえて、当該箇所から「経営者の直下で」を削除しました。
45	1. 本ガイドブックの位置づけ	３． 該当箇所　P1　２３行 企業がデジタル・トランスフォーメーション(DX)を推進する等 意見 デジタル・トランスフォーメーション（DX）はこれまで『データ利活用』と呼ばれてきたものと同義であれば、どこかでそれを明示して欲しい 理由 ・DXは近年のバズワードになっており、この用語を使う個人によって具体的に包含される意味合いが異なる。	該当箇所の箇条書きには括弧書きでDXの意味するところを記載しておりますが、御指摘を踏まえ、2.1の本文中で使用している箇所にも脚注5を追記しました。
46	3. 経営者が取り組むべき三要件	４． 該当箇所　P１３　７行 企業が一貫した姿勢で消費者のプライバシーを守っていくことは、個々のサービスや製品の品質を高めることと同じであり 意見 多分に重複する部分はあるものの、プライバシー保護と品質向上を同じであると断ずるのには違和感を覚える 理由 ・品質向上はそのサービスや製品を提供する企業の目線から見れば必要であるが、社会全体の観点からみれば必ずしも必要ではない。しかし、プライバシー保護は企業にとっての義務であり、社会全体が必要とするものである。	御指摘を踏まえて、該当箇所につき、「高めることと同じであり」を「高めることにつながり」へ修正させていただきました。
47	3.1. プライバシーガバナンスに係る姿勢の明文化	５． 該当箇所　P１５　４行 消費者のプライバシーを守っていくことが、商品やサービスの品質を向上させ 意見 上記と同様に、プライバシー保護と品質向上は繋がりうる、しかし、必然的にそうなるものではないため、この表現は誤解を招く。 理由 代替案としては、『品質』ではなく『ロイヤリティ（またはそれに該当する日本語）』または『利便性』とするのはどうか。例えば、本行であれば下記のようになる。 『消費者のプライバシーを守っていくことが、商品やサービスに対するロイヤリティを向上させ』 『消費者のプライバシーを守っていくことが、商品やサービスの利便性を向上させ』	「品質」は狭義には提供者が定めた仕様から逸脱していないという事ですが、現在は広い意味で捉えることが多く、例えば顧客（消費者）が求める特性全体をさすことも多いといえます。後者の使い方においてはご指摘いただいた「利便性」は含まれると解しています。 「利便性」は、商品・サービスの使い勝手に関わる特性ですが、適切なプライバシー保護は商品・サービスを使っているとき以外にも重要といえることから「利便性」に置き換えることは対象を限定しすぎることになると考えます。 「ロイヤリティ」（それに類する用語を含む）は顧客がその商品やサービスを継続的に利用するときの特性だが、このガイドブックでは、企業と顧客の関係性として、継続性がある場合だけでなく、一回切りの場合も対象となります。 以上より、「品質」との表現を使用させていただいております。
48	3.2. プライバシー保護責任者の指名	６． 該当箇所　P１６　８行 経営者による関与と明文化した内容の具体的な実践が不可欠である 意見 具体的に何を指すのか不明、『プライバシーへの取組み』か？しかし、『プライバシーへの取組み』は最低限に何を含むべきなのか明示すべき 理由 １７頁２行目に『姿勢を明文化した内容の実践』とある。	明文化した内容は、3.1に記載の「プライバシーガバナンスに係る姿勢の明文化」の内容を指しています。 ご指摘を踏まえて、該当箇所の文意が明確になるよう、修正しました。
49	3.2. プライバシー保護責任者の指名	７． 該当箇所　P１６　１０行 経営者は、組織全体のプライバシー問題への対応の責任者を担当幹部（以下「プライバシー保護責任者」という。）として指名し 意見 ・担当幹部というのが具体的にどのレベルの人間である必要があるのか明記すべき。そうしない場合、『経営者による関与』の実現は困難 ・レポートライン、独立性、兼任の受容性、求められる専門性や資質等の仔細を定めることで、名ばかりのプライバシー保護責任者が横行しないようにすべき ・とくに実際に事業の相談を経てプライバシーガバナンスを実践する現場担当者に指示をすることになるプライバシー保護責任者には、適切な指示を出すためにもある程度のプライバシー保護に関する専門性は絶対的に必要である。	プライバシー保護責任者は、一般データ保護規則（GDPR）でいうところの、利益相反規定において、強い独立性が担保されている、データ保護オフィサー（DPO: Data Protection Officer）とは必ずしも同じものとは限らず、役員が担うこともありうると脚注24に記載しております。 本ガイドブックの趣旨に照らして、個々の具体例については、企業の規模やリソースに応じた適用が認められるものであり、個々の企業の状況に応じて柔軟に利用していただきたいと考えております。 御指摘の点につきましては、本ガイドブックを公開後、各社の取り組みの収集を進め、更新を行っていきます。

DX企業のプライバシーガバナンスガイドブックver1.0（案）　パブリックコメントに対するご意見とご回答

ID	箇所	御意見の概要	回答
50	3.2. プライバシー保護責任者の指名	８． 該当箇所　Ｐ１６　フッター部分 強い独立性が担保されている、データ保護オフィサー（DPO: Data Protection Officer）とは必ずしも同じものとは限らず、役員が担うこともありうる 意見 GDPR の DPO も役員が担うことはありうると思われるため、訂正すべき。根拠は右記を参照。また『DPOと必ずしも同じものとは限らない』という部分を明示するためには、DPOとの相違点のリスト（または表）が一覧できると理解しやすい。DPOの要件が満たされた形でDPOの任命している企業は、DPOをプライバシー保護責任者とみなすだけで本ガイドブックの期待は満たしている、といえるのか。 理由 As a rule of thumb, conflicting positions within the organizations may include senior management positions (such as chief executive officer, chief operating, chief financial, chief medical officer, head of marketing department, head of human resources, or head of IT departments) but also other roles lower down in the organizational structure if such positions or roles lead to determine of purposes and means of processing. （DPO guidelines より引用） 『役員が担ってはならない』とは定められていない。あくまで、データの取り扱い目的や方法を決める立場にあるべきポジションや役割を除外しているに過ぎない。	ご指摘を踏まえて、脚注24に以下のとおり、追記しました。 「なお、ここでいうプライバシー保護責任者は、一般データ保護規則（GDPR）でいうところの、利益相反規定において、強い独立性が担保されている、データ保護オフィサー（DPO: Data Protection Officer）とは必ずしも同じものとは限らない。DPOは組織内において個人データの取扱いの目的及び方法を決めることにつながる地位（役員等）に就けないとされているが、プライバシー保護責任者は組織内において個人データ処理の目的及び手段を決定に関与する権限のある役職（役員クラス）から選任する方が機能する場合もあり得る。各組織に特有の組織構造に応じて、適切な立場からの者を指名することが望ましい。」
51	コラム	９ 該当箇所　Ｐ１１　６段落　３行目 協定で前もって合意した上で、提供したケースもあった 意見 政府が民間事業者にパーソナルデータの提供を求める際、政府が民間事業者に対して、プライバシーの保護等のために約束する事項を定め、それを企業に提示して、協定等を結ぶことを標準的な手順としていただきたい。 理由 提供の依頼だけが唐突に政府側から届き、民間事業者側が緊急に対応を協議しなければならくなるケースが生じないよう、民間事業者側の負担や、誤った判断をしてしまうリスクに配慮して、提供の意義・目的や必要となる制限事項等について政府側からまず具体的に提示いただきたい。	御指摘の点につきましては、今後の参考とさせていただきます。
52	4.1.2. プライバシー保護組織の役割	１０ 該当箇所　Ｐ１９　１７行目 専門的な知見を有する専任者を確保が困難な場合には、兼務の従業員のみで保護組織を構成するなど 意見 ・リソースの制約を盾に中身の伴わないプライバシーガバナンスが横行することを防ぐためにも、専門性を高める人材育成計画などを別途定めるべき。 理由 後に『プライバシー保護は高い専門性が必要な領域であることを念頭に置き、中長期的な視野に立ち、育成していく必要がある』と出てくるように、最初の取組みとして、専門性がない兼務者のみに構成となることは認めるべきである一方これを恒常的に認めるとプライバシーガバナンスのコンセプトが根底から瓦解しかねず、さらに明文化したプライバシーガバナンスを実践する実効性が低い。	御指摘を踏まえて、修正いたしました。
53	4.1.2. プライバシー保護組織の役割	１１ 該当箇所　Ｐ２０　１行目 図表７　プライバシー保護体制の構築 意見 複数人いる「経営者」がプライバシー保護責任者を任命するという図になっているが、プライバシー保護責任者はプライバシー保護のために必要があれば経営層の判断も制止し得るものでなくてはならないことの説明を追記すべき。 理由 新サービス等について、プライバシー保護責任者がリスクを指摘し、その実施を否認したにも関わらず、経営層に働きかけることによって実施可能となる、といったことが起きない体制とすべき	プライバシー保護責任者は、一般データ保護規則（GDPR）でいうところの、利益相反規定において、強い独立性が担保されている、データ保護オフィサー（DPO: Data Protection Officer）とは必ずしも同じものとは限らず、役員が担うこともありうると脚注24に記載しております。 また、「3.2.プライバシー保護責任者の指名」において、経営者は、プライバシー保護責任者から報告を求め、評価をすることで、組織の内部統制をより効果的に機能させる。その際には、プライバシー保護責任者の責任範囲を明確にし、プライバシー問題の発生を抑止するために必要な対応を遂行するための権限も与える必要があると記載しております。 御指摘の点につきましては、本ガイドブックを公開後、各社の取り組みの収集を進め、更新を検討していきます。
54	4.1.2. プライバシー保護組織の役割	１２ 該当箇所　Ｐ２０　９行目 さらに、見つかったプライバシー問題に対して (略) CS（カスタマーサービス）、政策企画などとの連携を図ることが重要である。 意見 この部分は、「4.1.3. 事業部門の役割」に含めるべき。 理由 事業部門が新サービス等を企画するにあたって、その内容に応じ情報セキュリティ部門やCS等と連携することはプライバシーリスクの有無に関わらず事業部門の責任として必須である。それは事業部門が責任を持って主導すべきであり、プライバシー保護組織がその責務を負うものであるかのように説明すべきではない。プライバシー保護を推進するためには、事業部門の自覚と主体的な行動が非常に重要である。	御指摘を踏まえて、事業部門の役割にも、自覚と主体的行動が重要である旨を追記しました。
55	ガイドブック全般	・３ページの１４行目「デジタル・トランスフォーメーション（DX）」は「DX」と記載したほうがよいと思います。前段の１ページの２４行目の枠内の１行目で略語の定義が記載されているから。 ・７ページの２行目「始まりつつある」と、４３ページの１４行目「はじめている」とは、どちらかに字句を統一したほうがよいと思います。 ・８ページの１３行目「以下、個人情報法」は「以下「個人情報法」という。」と記載したほうがよいと思います。７ページの１１行目と同様に。 ・８ページの２５行目「とおり」と、２７ページの７行目「通り」とは、どちらかに字句を統一したほうがよいと思います。 ・２１ページの１４行目「紐づけ」は「紐付け」と記載したほうがよいと思います。３ページの１２行目「名付け」等の例と同様に。 ・２６ページの６行目「当たって」と、３７ページの５行目「あたって」とは、どちらかに字句を統一したほうがよいと思います。	御指摘を踏まえて、修正いたしました。
56	ガイドブック全般	問題７：内部統制の限界 　「これら以外の公正な第三者の認証等として、セキュリティ管理に係る内部統制保証報告書」（「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（案）２０ページ）についても記載がございましたが、当意見全体で申し上げました様々なＩＳＭＳ、ＰＭＳ等の限界の問題と共通する要素も含まれていると考えられます、下記の「内部統制の限界」についてもご検討とご留意のほど、よろしくお願いいたします。ＩＳＭＳ、ＰＭＳ等の限界としても国、ＩＳＭＳ、ＰＭＳ等の規格関連機関、認証機関等から日本国民を含め、多くの方々への周知、注意喚起等の継続的実施を希望いたします。 引用文献 「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂について」 金融庁企業会計審議会（会長 徳賀 芳弘 京都大学副学長・教授　（令和元年１２月６日現在）） 「財務報告に係る内部統制の評価及び監査の基準」 ＵＲＬ　https://www.fsa.go.jp/news/r1/sonota/20191213.html	御意見は拝聴いたしました。
57	ガイドブック全般	問題８：組織の情報セキュリティの運用状態の経年劣化 　組織的には、最初は、良い状態でも、年数が経過するにつれ、巧妙なもみ消し方を覚え、状態が悪くなっていくおそれもございますので、ご検討とご留意のほど、よろしくお願いいたします。	御意見は拝聴いたしました。
58	ガイドブック全般	問題９：組織の情報セキュリティの教育が不十分である問題 　委託先、その再委託先等のＩＳＭＳ認証、ＰＭＳ認証等の取得の有無に拘らず、情報セキュリティに関する社内教育があると思いますが、細かなＩＳＭＳ、ＰＭＳ等に関する組織の内部規定については、しっかりと理解させる教育になっていない現状もございます。通報されるべき情報セキュリティの喪失、情報セキュリティ事象、情報セキュリティインシデント、情報事故等の定義、ＩＳＭＳ認証、ＰＭＳ認証等の適用範囲等すらも教育せず、曖昧な理解を社内に浸透させれば、通報されるべき問題をもみ消せる場合もございます。私は、情報セキュリティの資格もあり、在職時、社内規程も含めた、情報セキュリティの教育教材も作成しておりましたが、情報セキュリティの話をするだけで、上司（課長）が突然激昂し、怒鳴ってくることが度々ありました。雇止めの不利益も被っております。不可解で悪質な企業統治があります。 　現場で情報事故等が発生しても、現場の従業員、管理職等は、対応方法をそもそも理解していないので、規程を知らず、組織の不正な空気だけを読んだ、規程をまるで度外視、無視した杜撰な方法で対応する現状、迅速に適正な対応ができない場合等も憂慮しております。 　組織内のe-ラーニングもテキスト、動画等を読まず、機械的に次のチャプターへ移動する行為、理解度テストのカンニング等の不正な運用が実態として憂慮されます。ＩＳＭＳ、ＰＭＳ等のルールで、年1回以上の教育を実施していたとしても、前記の行為ができる曖昧な運用、悪しき組織内風土、従業員の倫理観の欠如、ＩＳＭＳ、ＰＭＳ等の目的から逸脱した運用、情報セキュリティ、法令、社内規程等を理解しない運用等は、システム障害、情報事故等の隠蔽に繋がり、ＩＳＭＳ、ＰＭＳ、内部統制上、問題があると存じます。e-ラーニング等で役員、現場管理職、従業員等の理解に繋がらない、手抜きの建前だけの教育をするのであれば、e-ラーニングの導入費用、導入時間、労働時間も無駄です。なお、私は、定期の理解度テストでカンニングせず満点合格しておりました。	御意見は拝聴いたしました。
59	3.2. プライバシー保護責任者の指名	合法のプライバシー問題は経営判断である。せっかく、プライバシー問題は経営者の責任・権限として定義しているのであれば、プライバシー保護責任者は経営権に関与できるレベル（役員クラス以上等）と踏むこむべきである。	脚注24に以下のとおり、追記しました。 「なお、ここでいうプライバシー保護責任者は、一般データ保護規則（GDPR）でいうところの、利益相反規定において、強い独立性が担保されている、データ保護オフィサー（DPO: Data Protection Officer）とは必ずしも同じものとは限らない。DPOは組織内において個人データの取扱いの目的及び方法を決めることにつながる地位（役員等）に就けないとされているが、プライバシー保護責任者は組織内において個人データ処理の目的及び手段を決定に関与する権限のある役職（役員クラス）から選任する方が機能する場合もあり得る。各組織に特有の組織構造に応じて、適切な立場からの者を指名することが望ましい。」 御指摘の点につきましては、今後の参考とさせていただきます。
60	3.2. プライバシー保護責任者の指名	内閣府が発表したSociety 5.0 リファレンスアーキテクチャより、情報の意味軸が定義されている。たとえば、監視カメラが問題であればアセット（カメラそのもの）なのかデータ連携（カメラの録画データ）なのか、データ（録画データのデータベース）なのか・・・プライバシー問題を情報の意味軸の権限・責任に応じて定義すべきである。	御指摘の点につきましては、今後の参考とさせていただきます。