個人情報保護委員会事務局（個人情報保護担当）宛

「個人情報の保護に関する法律についてのガイドライン（通則編、外国にある第三者への提供編、第三者提供時の確認・記録義務編及び匿名加工情報編）（案）」に関する意見

氏名	一般社団法人 電子情報技術産業協会
意見	
	1．通則編に関する意見 ＜意見１＞ ■該当箇所 10 ページ・4 行目等 ■意見 「個人識別符号」に該当することとなるものとして、「・・・顔の部位の位置及び形状から抽出した特徴情報を、本人を認証することを目的とした装置やソフトウェアにより、本人を認証することができるようにしたもの」と規定されているが、「認証する」ではなく「識別する」（identify）の用語を用いる方が適切であるため、修正していただきたい。 ■理由 本人を「認証する」という用語は、通常は「個人認証」（authentication）を意味し、本人が当の本人であることを他人に対して証明する行為（例えば、ログイン認証など）を指すため意味が異なると考える。 --- ＜意見２＞ ■該当箇所 27 ページ　法第 15 条第 2 項関係 ■意見 利用目的の変更が許容される「本人が通常予測し得る限度と客観的に認められる範囲」に該当する事例、該当しない事例を例示していただきたい。 ■理由 経済産業分野ガイドラインでも事例が記載されており、法改正の際も事業者の関心が高かった部分である。ガイドラインへの記載が困難であれば、Ｑ＆Ａや解説資料への記載でも構わないので、可及的速やかに公開していただきたい。

＜意見３＞
■該当箇所
43 ページ・11 行目

■意見
委託先における個人データの取扱状況を把握するため、「定期的に監査を行う等」が要求されているが、監査の必要性については、個人データが漏洩等をした場合に本人が被る権利利益の侵害の大きさを考慮すべきである。委託業務の性質及び規模、個人データの取扱状況、個人データを記録した媒体の性質等に起因するリスクに応じて判断すべきものであるため、「リスクに応じて」といった文言を追加していただきたい。

■理由
委託先における個人データの取扱状況の把握のためには、委託業務の性質及び規模に応じて、監査以外の方法も考えられるところであり、委託元及び委託先の合意のもと、適切な手法を選択するべきものと考える。本ガイドラインにおいて一律に監査を必要とすると、いかなる委託業務においても監査の実施及び受け入れが必要であるかのような過剰反応を惹起しかねないため。

＜意見４＞
■該当箇所
79 ページ・1 行目

■意見
漏洩等の事案が発生した場合における個人情報取扱事業者が実施することが望まれる対応については、別に定めることとされているが、権限一元化の趣旨を踏まえ、複数の行政機関からの重複した報告・説明の聴取等がなされないよう、漏洩等の事案が発生した場合における行政機関への報告窓口等を一元化していただきたい。

■理由
複数の行政機関から重複した報告・説明の聴取等がなされると、事業者にとっては過重な負担となるため。

＜意見５＞
■該当箇所
87 ページ・1 行目

■意見
個人データの適正な取扱いの確保について組織として取り組むために、基本方針を策定することが求められているが、この基本方針は、従来の経済産業分野ガイドラインで規定されている「個人情報保護を推進する上での考え方や方針（いわゆる、プライバシーポリシー、プライバシーステートメント等）」と同じもので良いのか、明確化していただきたい。

■理由
個人情報取扱事業者は、現行法の下においても、法 27 条及び 35 条に関連して、個人情報保護を推進する上での考え方や方針（いわゆる、プライバシーポリシー、プライバシーステートメント等）を策定し、外部に公開していることが一般的となっているが、本ページにいう「基本方針」が、これらプライバシーポリシー等と同一のものを指しているのか、または、プライバシーポリシー等に加えて基本方針を作成することが要求されているのか、あるいは、個人データの取扱に係る事業者の内部的規律の原則を定めることを求められているのか、必ずしも明らかではないため。

	＜意見６＞ ■該当箇所 97 ページ　技術的安全管理措置の手法の例示 ■意見 現在、経済産業分野ガイドラインに記載されている技術的安全管理措置の手法の例示については、原則として、全て記載して（継続して）いただきたい。全ての記載が困難な場合には、「どの手法がどの表現に包含されているか」を明確にしていただきたい。 ■理由 現行の経済産業分野ガイドラインに記載されている技術的手法の例示は、10 年余りにわたる個人情報保護法施行のノウハウの蓄積とも言え、多くの個人情報取扱事業者にとって、技術的対策を実施する上で貴重な手がかりとなっている。 今回提示されたガイドラインでは、技術的表現(テクニカルターム)の多くが削除され、情報システムにセキュリティ対策を実施する側にとっては、どのような技術的対策を実施したらよいか、判然としない記載となっている。 ガイドラインへの記載が困難な場合には、参考資料などの位置づけでもよいので、現行の経済産業分野ガイドラインに記載されている技術的手法の例示が抜けないよう、配慮いただきたい。

2. 外国にある第三者への提供編に関する意見

＜意見１＞
■該当箇所
4 ページ　図：法第 23 条と第 24 条の適用関係

■意見
図表内のハイフン（ー）の意味している内容が理解しにくく明確化すべきと考える

■理由
「オプトアウト手続」の行のハイフンは「該当ケースなし（第 24 条の要件を満たすには本人同意以外の方法が必要）」という意味であるが、「例外」の行のハイフンは「第 23 条の例外に該当すれば、第 24 条の要件は不要」という意味であり、両者で意味が異なるため。

＜意見２＞
■該当箇所
ページ・5 行目

■意見
外国法人が日本国内のデータセンタ運営事業者との契約等に基づき、日本国内のデータセンタを利用することがある。そのような外国法人に対し、もっぱら日本国内のデータセンタに個人データを保存することを前提として個人データを提供する場合、すなわち本邦の域外に個人データが物理的に移転することを前提としていない場合には、単に個人情報取扱事業者の義務が適用され、法第 24 条（外国にある第三者への提供の制限）の適用はないということを明らかにしていただきたい。

■理由
「外国にある第三者」該当するか否かは、別の法人格を有するかどうかにより判断されるとのことであるが、上記意見のように、本邦の域外に個人データが物理的に移動することのない場合においても、別の法人格を有している場合には法 24 条の適用があるのかどうか明らかにするため。

＜意見３＞
■該当箇所
5 ページ　2-2　外国にある第三者

■意見
海外にあるクラウドに個人情報を保管する場合でも、海外事業者は個人情報にアクセスできず、国内の個人情報取扱事業者しかアクセスできないよう適切に安全管理措置が実施されている場合は、「外国にある第三者への提供」に該当しないことを明確にしていただきたい。

■理由
現在、上記意見欄に記載したような海外(特に米国系 IT 企業が運営する)の安全なクラウド利用が一般化している。このような利用に過重な負担を課すと、IoT 推進に大きなマイナスとなる事態が懸念される。ガイドライン本文への記載が困難であれば、Q&A 等による明確化でも構わない。

＜意見４＞
■該当箇所
7 ページ～8 ページ

■意見
外国事業者が「OECD プライバシーガイドライン」に準拠していることが、規則第 11 条 1 号「個人情報取扱事業者と個人データの提供を受ける者との間で、当該個人データの取扱いについて、適切かつ合理的な方法により、法第 4 章第 1 節の規定の趣旨に沿った措置の実施が確保されていること。」の条件を満たすとの判断であれば、その旨明記していただきたい。
なお、これに該当する場合、契約等において「OECD プライバシーガイドライン」準拠であるとの記載があればよいのか、明らかにしていただきたい。

■理由
事業者による当ガイドライン記載内容の判断に差異が生じないようにするため。

＜意見５＞
■該当箇所
31 ページ
3-3　個人データの提供を受ける者が、個人情報の取扱いに係る国際的な枠組みに基づく認定を受けていること（規則第 11 条第 2 号関係）

■意見
「国際的な枠組みに基づく認定」に関し、例示を一つにとどめず、複数ご提示いただきたい。グローバルにビジネスを展開している IT 企業にとっては、ISO/IEC27000 シリーズのような国際標準も有効と考える。

■理由
現状、APEC の CBPR 認証を受けている企業は極めて限定されている。それに対し、ISO/IEC 27000 シリーズは情報セキュリティ管理の国際規格として広く受け入れられており認証を取得している企業も多い。最近では ISO/IEC 27018 のように、個人情報を保管するクラウドに適合した規格も誕生している。是非、国際的に広く認められている認証制度を取り入れていただきたい。

3. 第三者提供時の確認・記録義務編に関する意見

＜意見１＞
■該当箇所
12 ページ・最終行～13 ページ・3 行目

■意見
「個人データが適法に入手されたものではないかと疑われる場合に」（2 ヵ所あり）を次のように修正していただきたい。
⇒「個人データが適法に入手されたものではないと疑われる場合に」または
「個人データが不正に入手されたものではないかと疑われる場合に」

■理由
文理解釈上、意味が逆になっていると思われるため。
なお、13 ページ・下から 2 行目では、「個人データが適法に入手されたものではないと疑われるにもかかわらず」と適切な表現になっている。

＜意見２＞
■該当箇所
16～17 ページ
4-1-2-2　一括して記録を作成する方法（規則第 12 条第 2 項、第 16 条第 2 項関係）

■意見
一括記録作成時に、提供先/提供元が法人である場合は、法人の代表者氏名を記録する必要はなく、法人番号または本店所在地と法人名称など、提供先／元の法人が特定できる情報が記載されていれば十分であることを明確にしていただきたい。

■理由
特定の法人間で継続的に提供/受領を行う場合、実務上、代表者の交代について確実にフォローし正しく記録することは事業者にとって過重な負担である。（手順やルールを定めても、漏れが出ることが予想される。）
法 25 条 1 項(記録義務)は、「第三者の氏名または名称」
規則第 13 条 1 項ロは、「名称その他の当該第三者を特定するに足りる事項」
という定めであり、法人の代表者氏名の記録義務はないことを明確にしていただきたい。

＜意見３＞
■該当箇所
27 ページ・下から 7 行目

■意見
「記録事項の内容は同一でなければならないため、例えば、同一法人であっても、代表者が交代し、その後に記録を作成する場面では、改めて、新代表者の氏名について記録をしなければならない。」とあるが、提供先/提供元が法人である場合は、法人の代表者氏名を記録する必要はなく、法人番号または本店所在地と法人名称など、提供先／元の法人が特定できる情報が記載されていれば十分であることを明確にしていただきたい。

■理由
特定の法人間で継続的に提供/受領を行う場合、実務上、代表者の交代について確実にフォローし正しく記録することは事業者にとって過重な負担である。（手順やルールを定めても、漏れが出ることが予想される。）

	＜意見４＞ ■該当箇所 全般 ■意見 第三者提供時の確認・記録義務は、名簿業者以外の一般事業者にとっては特別な記録を作成する必要はなく、日常の事業活動の中で発生する記録類（伝票・ログ・メール等）を一定期間(1～3 年間)保存し、個人情報保護委員会から照会等があった場合には、個人情報の提供先/提供元を説明できればよい主旨をわかり易く周知・広報していただきたい。 ■理由 法令の規定/ガイドラインの記載は、法律用語による記述で全般に難解である。本来の主旨である「名簿業者のトレーサビリティ確保」の目的が不明確となって、一般事業者に「過剰反応」を起こすおそれが高いため。

	4. 匿名加工情報編に関する意見 ＜意見１＞ ■該当箇所 3 ページ　2　定義 ■意見 　平成 28 年 8 月経済産業省発行「匿名加工情報作成マニュアル」では「個人識別に係るリスク低減」を対象にしているのに対し、本ガイドラインでは「特定の個人を識別できないようにする加工」を対象にしているため、対象範囲が異なるように読み取れる。事業者の混乱を招く。匿名加工事業者は本ガイドラインに準拠すればよいということであれば、経済産業省発行「匿名加工情報作成マニュアル」の位置づけを明確にしていただききたい。 ■理由 　事業者の判断により、匿名加工基準に差異が生じるため。 ---------- ＜意見２＞ ■該当箇所 19 ページ～21 ページ ■意見 　匿名加工情報の作成時の公表、および第三者へ提供時の公表は、両者を包括的に公表できることを明確にしていただきたい。 ■理由 　事業者の判断により、公表時の対応に差異が生じるため。 以　上