資料２－２

「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（案）」に関する意見募集の結果について

平成29年２月16日
個人情報保護委員会事務局

個人情報保護委員会においては、平成28年12月８日（木）から本年１月６日（金）まで、「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（案）」につきまして、広く国民の皆様からの御意見を募集しました。

その結果、この意見募集に対して33の個人又は団体から延べ117件の御意見等が寄せられ、これら御意見等に対する当委員会の考え方について、別紙のとおり取りまとめました。

また、お寄せいただいた御意見等を踏まえた上で、本日、「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」を定め、個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律（平成27年法律第65号）の施行の日（平成29年５月30日）から施行することとなりましたのでお知らせします。

御意見をお寄せいただいた皆様に感謝申し上げるとともに、引き続き、当委員会の活動に御理解と御協力をいただきますようお願い申し上げます。

「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（案）」に関する意見募集結果

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
1	全般	・本告示につき中小規模事業者への配慮はないのか，回答されたい。もし存在しないのであれば，そのような通則編とは異なる扱いが正当化される理由を説明されたい。特にそのようなやり方が中小規模事業者の円滑な改正法対応を要求する法附則１１条に違反しない理由を説明されたい。（なお，特定個人情報告示特２（２）と平仄をあわせる意味でも，中小規模事業者への配慮規定を入れるべきである。） 【金融機関における個人情報の実務研究会】	「事業者における特定個人情報の漏えい事案等が発生した場合の対応について（平成 27 年特定個人情報保護委員会告示第２号）」においては、個人情報取扱事業者以外の事業者のみを対象として、個人情報保護委員会への報告を要しない場合に係る要件を規定しているところ、本告示においては、中小規模事業者を含むすべての個人情報取扱事業者を対象として、当該要件よりも広い概念で、個人情報保護委員会等への報告を要しない場合の要件として規定しています。
2	対象とする事案	・本告示では，特定個人情報の漏えい事案等が発覚した場合については，本告示によらず，特定個人情報告示によるとあるが，①事業者の保有する情報のうち確実に特定個人情報は漏えい等したが，本告示１で定義される漏えい等事案かは不明である場合，②確実に本告示１で定義される漏えい等事案であるが，特定個人情報が漏えい等したか不明である場合，③確実に本告示１で定義される漏えい等事案でありかつ確実に特定個人情報も漏えい等している場合，④事業者の保有する情報のうち何かが漏えい等していることは確実だが，その情報に特定個人情報が含まれるかも不明であれば，本告示１で定義される漏えい等事案かも不明である場合，⑤そもそも事業者の保有する情報について漏えい等しているかが不明であり，その情報に特定個人情報が含まれるかも不明であれば，本告示１で定義される漏えい等事案かも不明である場合のそれぞれについて，本告示と特定個人情報告示のいずれが適用されるかそれぞれ理由を付して回答されたい。（１つの事件で特定個人情報とそれ以外の個人情報が同時に漏えいすることは頻繁に起こり得るが，その場合には特定個人情報告示のみで処理され，本告示は一切関係がないのか，そのような場合には，特定個人情報の漏洩部分について特定個人情報告示で処理し，それ以外の部分について本告示で処理するのかといった「振り分け」が不明確なので質問させて頂いている。） 【金融機関における個人情報の実務研究会】	個人データ（特定個人情報に係るものを除く。以下同じ。）又は加工方法等情報及び特定個人情報の双方が漏えい、滅失若しくは毀損し又はこれらのおそれが生じたという事案については、個人データ又は加工方法等情報について本告示が、特定個人情報について「事業者における特定個人情報の漏えい事案等が発生した場合の対応について」（平成 27 年特定個人情報保護委員会告示第２号）が、それぞれ適用されます。御指摘の①から⑤までにおいて漏えい等が確定している場合には当該情報に係る告示が適用されます。また、「（漏えい等しているか）不明」の意味が必ずしも明らかでありませんが、漏えい等のおそれがある場合には当該漏えい等のおそれのある情報に係る告示が適用されるものと考えられます。
3	対象とする事案	・本告示１につき，通則編４で「「漏えい等」とは，漏えい，滅失又は毀損のことをいう」と明確に定義され，それを前提に本告示に委任している。ところが，本告示では，「個人情報取扱事業者が保有する個人データ(特定個人情報に係るものを除く。)の漏えい，滅失又は毀損」（本告示１（１））だけではなく「個人情報取扱事業者が保有する匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号(特定個人情報に係るものを除く。)並びに個人情報の保護に関する法律(平成 15 年法律第 57 号。以下「法」という。)第 36 条第１項の規定により行った加工の	本告示においては、御指摘のように「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）」４．における「漏えい等（※）の事案が発生した場合等」（個人データの漏えい、滅失又は毀損）とともに、個人情報取扱事業者として適切な安全管理措置を講ずべき匿名加工方法に関する加工方法等情

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		方法に関する情報(以下「加工方法等情報」という。)の漏えい」（本告示１（２））やそれらの「おそれ」（本告示１（３））までが対象となっているところ，この範囲まで本告示の対象に含めることがなぜ正当といえるのか説明されたい。 【金融機関における個人情報の実務研究会】	報の漏えい等についても規定することとしています。
4	対象とする事案	・本告示１（１）につき「漏えい」とは何か，定義を回答されたい。例えば，第三者提供の際に法令違反がある場合全て「漏えい」か，それともその一部か，はたまたそれが違法であっても第三者提供の場合は「漏えい」ではないのか等を明確に回答されたい。通則編パブコメ３５６番等からは個人情報取扱事業者が意図せず第三者がアクセス可能になった場合には「漏えい」だという趣旨と理解されるが，例えば個人情報取扱事業者の権限ある役職員が法２３条の制限に違反して顧客名簿を第三者に売却したという場合，これが「漏えい」なのか確認されたい。また，個人情報取扱事業者の権限なき役職員が法２３条の制限に違反して顧客名簿を第三者に売却したという場合はこれが「漏えい」なのか確認されたい。 【金融機関における個人情報の実務研究会】	一般的に現状の案で御理解いただけるものと考えます。個人情報取扱事業者が意図せず第三者にアクセスされた場合と異なり、個人情報取扱事業者が売却などにより自らの意図に基づき個人データを第三者に提供する場合には「漏えい」には該当しないものと考えられます。
5	対象とする事案	・本告示１（１）につき「滅失」とは何か，定義を回答されたい。例えば，個人データそのものは何ら変わらず個人情報取扱事業者の手元に存在するが，その媒体にかけていたパスワードを忘れてしまい全くアクセスできなくなった場合，これは「滅失」といえるか，回答されたい。また，例えば個人の氏名データのうち「姓」だけがなくなり，「名」だけが残っているというようなデータの「一部」が存在しなくなった場合についてこれは「滅失」か「毀損」か（はたまたそれ以外か）回答されたい。一部滅失という概念は存在するのか，それともそのような概念は存在せず，一部がなくなった場合であればすべて「毀損」と解すべきか，回答されたい。 【金融機関における個人情報の実務研究会】	ある事案が「滅失」又は「毀損」のいずれに該当するかについては、対象の情報の内容・性質等の事情を勘案して、個別の事例ごとに判断することとなります。漏えい等事案に該当する場合には、個人情報取扱事業者において本告示２．の措置を講じることが望ましく、また、本告示３．(2)に該当する場合を除いて、個人情報取扱事業者は、個人情報保護委員会等への報告に努めることが求められます。
6	対象とする事案	・本告示１（１）につき「毀損」とは何か，特に「滅失」との相違に照らして定義を回答されたい。例えば，個人データとして顧客名簿.xls と従業員名簿.xls という２つのファイルがあった場合において，顧客名簿.xls を誤って削除してしまったとすると，これは「滅失」であって「毀損」ではないということでいいか，確認されたい。では，RDB（リレーショナルデータベース）において，顧客について顧客用のログインパスワードとユーザーID（キー）が入っているテーブルＡと顧客氏名とユーザーID（キー）が入っているテーブルＢがあった場合に，テーブルＡの情報を誤って削除してしまった場合も同様に「滅失」であって「毀損」ではないということでいいか，確認されたい。 【金融機関における個人情報の実務研究会】	ある事案が「滅失」又は「毀損」のいずれに該当するかについては、対象の情報の内容・性質等の事情を勘案して、個別の事例ごとに判断することとなります。漏えい等事案に該当する場合には、個人情報取扱事業者において本告示２．の措置を講じることが望ましく、また、本告示３．(2)に該当する場合を除いて、個人情報取扱事業者は、個人情報保護委員会等への報告に努めることが求められます。
7	対象とする事案	・本告示１（１）につき，例えば（コンピュータシステム上の）個人情報データベース等にシステム障害が発生し長期間に渡って個人データを利用できないという事態は個人データの可用性に少なからぬ影響を与えるが，このような場合については，本告示でいう「漏えい等」に該当しないということでいいか，確認されたい。その上で，個人データのＣ（機密性）Ｉ（完全性）Ａ（可用性）に関する事項のうち，なぜ本告示は「漏えい，滅失又は毀損」のみを取り上げ，それ以外を取り上げないのか，	御理解のとおりです。改正後の法第 20 条の趣旨に照らして、「個人データの漏えい、滅失又は毀損」を本告示の対象とする事案として規定しています。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		説明されたい。 【金融機関における個人情報の実務研究会】	
8	対象とする事案	・本告示１（１）につき「個人データ」に限定しているが，「個人情報」であっても，それが漏えいした場合に大きな影響を与えるものは存在する。例えば（散在情報であって個人データではない）要配慮個人情報の漏えいや，（散在情報であって個人データではない）クレジットカード情報の漏えい等は，個人データの漏えいと同程度，場合によってはそれ以上の影響を与えると解されるが，このような場合については本告示が適用されないということでよいか，確認されたい。 【金融機関における個人情報の実務研究会】	個人情報データベース等の一部を構成しない個人情報の漏えい、滅失又は毀損は、本告示が対象とする事案には含まれません。
9	対象とする事案	・本告示１（２）につき「個人情報取扱事業者が保有する匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号」というのは，当該「記述等及び個人識別符号」が当該匿名加工情報と紐づく形で漏えい等した場合にのみ本告示を適用するということでよいか回答されたい。例えば，顧客Ａの購買履歴からＡの氏名及び住所を削除して匿名加工情報Ｂを作成し，これを公衆に対して販売しているいう場合において，Ａの氏名及び住所が漏えいしたが，それはあくまでも個人情報（散在情報）としてのＡの氏名及び住所が漏えいしただけで，匿名加工情報Ｂを作成する際に削除された情報であることが知られていないという場合には，漏洩したのは個人データではなく，また「記述等及び個人識別符号」が当該匿名加工情報と紐づく形で漏えい等しているわけではないので，本告示は適用されないということでよいか，確認されたい。 【金融機関における個人情報の実務研究会】	個別の事例ごとに判断されることとなりますが、一般に漏えい等事案に係る情報が、匿名加工情報の作成に用いた個人情報から削除された記述等及び個人識別符号であり、加工方法等情報と推定し得る場合には、本告示の対象となります。
10	対象とする事案	・本告示１（２）の「個人情報取扱事業者が保有する匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号」につき，法３６条では，「匿名加工情報」について，「匿名加工情報データベース等を構成するものに限る」と限定しているところ，本告示１（２）の「匿名加工情報」についてそのような限定が付されるのか，回答されたい。つまり散在情報である匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号については，法３６条２項においては安全管理措置が必要とされていない以上，本告示の対象とされないと思われるが，そのような理解でよいか回答されたい。 【金融機関における個人情報の実務研究会】	御理解のとおりです。なお、御意見を踏まえ、本告示１．(2)を次のとおり修正します。 「個人情報取扱事業者が保有する加工方法等情報（個人情報の保護に関する法律施行規則（平成 28 年 10 月５日個人情報保護委員会規則第３号）第 20 条第１号に規定する加工方法等情報をいい、特定個人情報に係るものを除く。）の漏えい」
11	対象とする事案	・本告示１（２）の「個人情報取扱事業者が保有する匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号」につき，「年齢のデータを 10 歳刻みのデータに置き換えた」というような復元につながらない情報（匿名加工情報編ガイドライン 3-3-1*参照）が漏えいした場合には本告示の対象とされないと思われるが，そのような理解でよいか回答されたい。 【金融機関における個人情報の実務研究会】	御理解のとおりです。なお、御意見を踏まえ、本告示１．(2)を次のとおり修正します。 「個人情報取扱事業者が保有する加工方法等情報（個人情報の保護に関する法律施行規則（平成 28 年 10 月５日個人情報保護委員会規則第３号）第 20 条第１号に規定する加工方法等情報をいい、特定個人情報に係るものを除く。）の漏えい」
12	対象とする事	・本告示１（２）の「加工方法等情報」につき規則２０条は「その情報を用いて当該個人情報を復元	御理解のとおりです。なお、御意見を踏まえ、本

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
	案	することができるものに限る」との限定を付しているところ，本告示１（２）の「加工方法等情報」についてそのような限定が付されるのか，回答されたい。つまりその情報を用いて当該個人情報を復元できない加工方法等情報については，規則２０条においては安全管理措置が必要とされない以上，本告示の対象とされないと思われるが，そのような理解でよいか回答されたい。 【金融機関における個人情報の実務研究会】	告示１．(2)を次のとおり修正します。 「個人情報取扱事業者が保有する加工方法等情報（個人情報の保護に関する法律施行規則（平成 28 年 10 月５日個人情報保護委員会規則第３号）第 20 条第１号に規定する加工方法等情報をいい、特定個人情報に係るものを除く。）の漏えい」
13	対象とする事案	・本告示１（３）の「おそれ」とは何か，定義を回答されたい。例えば，個人情報取扱事業者が個人情報をインターネットにつながったパソコン・サーバー上で保管している場合，常に第三者からの不正アクセス等による漏えいの抽象的可能性は否定できないが，これは本告示１（３）でいう「おそれ」なのか回答されたい。それとも，「何かの情報が漏えいしたことは間違いないが，その情報が何か分からず，個人データが含まれる可能性を否定できない」という程度ではじめて「おそれ」があるのか，「おそれ」といえるのがどのレベルに至った場合なのかを回答されたい。 【金融機関における個人情報の実務研究会】	「おそれ」の該当性については、個人データ等に関して生じた事象等の事情を勘案して個別の事例ごとに判断することとなりますが、一般的には、個人データの漏えいが疑われるものの確証がないといった場合が該当すると考えられます。
14	対象とする事案	・本告示１につき，単なる個人情報保護法違反の事実があっただけでは漏えい等事案には該当しないことを確認されたい。特定個人情報告示では，「漏えい事案その他の番号法違反の事案又は番号法違反のおそれのある事案が発覚した場合」として，法違反全般を対象としているが，なぜマイナンバー法と個人情報保護法で取扱いを異にするのか，その理由を回答されたい。合理的理由がなければ平仄を取った修正を行われたい。 【金融機関における個人情報の実務研究会】	個人データについて、特定個人情報に比して、取扱いの態様、取り扱われる情報の内容・性質等が多岐に亘り、これに伴い法違反の態様も多様なものが想定されるところ、それらすべてについて告示において個人情報取扱事業者が講じることが望まれる措置及び努めるべき事項を規定することは、軽微な事案を含めて基本的に逐一報告を求める形として告示を定めることとなります。改正後の法においては、これまで個人情報保護法の適用がなかった 5,000 人分以下の個人情報を取り扱う小規模の事業者も新たに対象となり、全ての事業分野における個人情報取扱事業者が対象となるところ、個人情報取扱事業者に過度の負担を課すこととなり、適切でないと考えます。
15	対象とする事案	対象とする事案として「個人情報取扱事業者が保有する個人データの・・・」とありますが、要配慮個人情報についても、「個人データとなっている要配慮個人情報」のみが対象と考えて良いのでしょうか？ 通則編ガイドラインのパブコメにおいて、「要配慮個人情報は、オプトアウトによる第三者提供はできない。」となっているのは間違えで、「個人データのうち要配慮個人情報は、オプトアウトによる第三者提供はできない。」が正解ではないかと質問させていただいたところ、「一般的に現状の案で御理	本告示において対象とする事案は、御理解のとおり、要配慮個人情報についても、個人データに該当する要配慮個人情報のみとなります。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		解頂けるものと考えます。」と回答がありました。 理解できないので明確な回答をお願いいたします。 【改正個人情報保護法　消費者志向で考える事業者ガイドライン研究会】	
16	対象とする事案	対象とする事案として「個人情報取扱事業者が保有する個人データの・・・」とありますが、購買履歴については、「個人データの定義」を満たすかどうかで個別に判断されるものとなるということでしょうか？ 法第２条第１項第１号の「個人情報」に該当する要件は、 (1)生存する「個人に関する情報」であること。 (2)特定の個人を識別することができるものであること。 ですが、「購買履歴」や「位置情報」が個人情報となるかどうかは、ここ 12 年で浮上した疑問が集中するところとなっています。 「上記の(1)及び(2)に該当する情報」と組み合わせた情報については、その全体が「個人情報」となるかを理解することが難しいため、漏えい事案の対象となるかどうかも理解しづらくなっています。 鈴木　●郎ー購入：商品Ａ ←「単独の購買情報：商品名」では同じ商品を購入した者が複数人いると、他の情報と容易に照合できないので「商品Ａ」は個人情報ではない。 そのため漏えいしたのが、「顧客マスター」ではなく「購買マスター」の方で、かつ顧客番号など「他の情報と容易に照合することができるもの」を含まない「商品Ａ」だけの購買情報であった場合には、同じ購買履歴を示すものがいるかどうかを確認し、同じ購買履歴を示すものが複数人いた場合には、「他の情報と容易に照合することができ」にはならず、そのため特定の個人を識別することができることとはならないので、個人情報には該当せず、個人データではないので、ここでいう対象となはならい。 一方で、 購買情報のみであっても、漏えいしたのが「商品Ａ，商品Ｂ」であった場合で、その両方を購入した人が購買マスターから１名のみしか見つからなかった場合で、事業者内部ではそこから顧客ＩＤを引っ張ってくることができるという場合には「他の情報と容易に照合することができ」に当たり、それにより特定の個人を識別することができることとなるため、個人情報に該当し、個人データとなる場合がある。 この場合にはたとえ漏えいしたのが「商品Ａ，商品Ｂ」という情報のみであっても、対象となるという理解で宜しいでしょうか？ 【改正個人情報保護法　消費者志向で考える事業者ガイドライン研究会】	本告示は、個人情報取扱事業者において保有されている個人データの漏えい等があった場合を対象としています。 個別の購買履歴が個人データに該当するかどうかについては、本意見募集の対象外と考えます。一般論としては、購買商品情報が当該商品を購買した顧客情報と結びついている場合、当該個人データの一部である場合が多いものと考えられます。
17	対象とする事	（該当箇所）	御理解のとおりです。改正後の法第 20 条の趣旨

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
	案	パブリックコメントが行われている告示案全体 （意見） 当該告示案は、「個人データの･･･」と明示していますが、これは、個人情報取扱事業者が個人情報データベース等を構成していない個人情報を漏えい等した場合については対象にはならないという理解でよいでしょうか。個人データに限定する理由はどのようなことでしょうか。 （理由） 個人情報データベース作成以前の原資料を移送時に紛失し漏えいするような事案が現実に起きています。また、「3.(2) ②」にある荷物の宛名は、個人データではなく、個人情報であるケースもあると考えられます。 【一般財団法人日本情報経済社会推進協会】	に照らして、「個人データの漏えい、滅失又は毀損」を本告示の対象とする事案として規定しています。
18	対象とする事案	（該当箇所） 1ページ、　5行目から6行目、および「1．対象とする事案」部分 （意見） 「個人データの漏えい、滅失または毀損」、「匿名加工情報の漏えい」という安全管理措置に係るものに限定されています。一方で、前書きに記されている「二次被害の防止、類似事案の発生防止等」が必要という観点からは、目的外利用等を含む「規定違反」も対象に入れる必要があるのではないでしょうか。 （理由） 現実には、例えば、作業担当者が荷物の受取人に好意を持ち、宛名情報を持ち出し（規定違反）、業務以外の目的で連絡をとるなどの事案も見られます。 【一般財団法人日本情報経済社会推進協会】	本告示は、御理解のとおり、改正後の法第 20 条及び第 36 条第 2 項に関連して事業者が講ずることが望ましいと考えられる措置（対応）について規定しています。
19	対象とする事案	■該当箇所 1 ページ・下から 8 行目 他 ■意見 全般に文章が難解だが、特に 1(2)の表記が分かりにくい。 例えば、「法」を予め前文で定義した上で、以下のように表記すると分かりやすくなるのではないか。 (2)　個人情報取扱事業者が保有する「加工方法等情報」の漏えい （なお「加工方法等情報」とは、以下の情報をさす ・匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号（特定個人情報に係るものを除く。） ・法第 36 条第 1 項の規定により行った加工の方法に関する情報） ■理由 原案では１文が長すぎ、法律の専門家ではない一般人の読解力では、正しく理解することが	御意見を踏まえ、本告示１．(2)を次のとおり修正します。 「個人情報取扱事業者が保有する加工方法等情報（個人情報の保護に関する法律施行規則（平成 28 年 10 月５日個人情報保護委員会規則第３号）第 20 条第１号に規定する加工方法等情報をいい、特定個人情報に係るものを除く。）の漏えい」

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		困難な文章となっているため。 【一般社団法人　電子情報技術産業協会】	
20	対象とする事案	○意見１ （該当箇所）１ページ　１ 対象とする事案 （意見内容）ガイドライン（通則編）では、「漏えい等」とは、漏えい、滅失又は毀損のことをいうと規定されているが、本告示においては、「紛失」（誤廃棄した確信が持てず、行方不明の場合）も「漏えい」に含まれるのかを追記して頂きたい。 （理由）「紛失」事案が対象か否かにより実務影響が相違するため。対象は「個人データ」ではなく、「個人情報」の場合の「紛失」を想定。 【日本クレジットカード協会】	「紛失」は、一般的に、「漏えい」又は「滅失」のいずれかに該当し、対象の情報が保管されていた状況等の事情を勘案して個別の事例ごとに判断されることとなります。なお、個人データに該当しない個人情報の漏えい、滅失又は毀損は、本告示が対象とする事案には含まれません。
21	対象とする事案	（該当箇所）３ページ （2）報告を要しない場合　実質的に個人データ又は加工情報等情報が外部に漏えいしていない場合 （質問および要望） 質問４：「個人データの漏えい等の事案が発生した場合」には、どのような場合が含まれますでしょうか。インターネット公衆回線を用いた場合の個人情報データの送信において以下の想定事例について、ご見解をお知らせください。 想定事例１：インターネットではバケツリレー方式でインターネット事業者間でのデータを転送しています。公衆回線（LAN など）に生体識別データ（登録用生体識別データ、照合用生体識別データ）、免許証番号、銀行口座番号、携帯電話番号などを流す場合これらのいずれかのデータをインターネット上に流すこと自体が漏えいにあたりますでしょうか。何故ならば、個人情報データが各インターネット事業者の間をパケットデータとして、バケツリレー方式で転送されるためです。 想定事例２：TLS のような仕組みを用いてエンドツーエンドでの暗号化通信が行われている場合は漏えいにあたらないとの解釈でよろしいでしょうか。 想定事例３：通信事業者が悪意を持って無断でパケットを記録した場合、これは漏えいにあたりますでしょうか。 漏えいに、第三者がデータとして収集できることが含まれますでしょうか。漏えいの定義に関するご見解を頂きたいと思います。 質問５：質問４の想定事例３は、一般の事業者は対策が不可能と思われますが、どこまでが事業者で	いずれの場合も、個人情報取扱事業者が、その意図に基づいて個人データ等を外部に送信する場合のことであり、漏えい等事案には該当しないものと考えられます。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		行うべき安全措置の義務となるでしょうか。 質問６：ネットワーク、特にインターネット（公衆回線）で個人情報を送る場合に、VPN 通信を用いて個人情報を含むデータが送られている場合は、各インターネット事業者の間を経由してパケットデータとして送られたとしても「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断」されるとの認識でよろしいでしょうか。 質問７：ネットワーク、特にインターネット（公衆回線）で暗号化して個人情報を送る場合には、各インターネット事業者の間を経由してパケットデータとして送られたとしても「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断」されるとの認識でよろしいでしょうか。 質問８：ネットワーク、特にインターネット（公衆回線）で個人情報を送る場合に TLS 通信を行うことで、各インターネット事業者の間を経由してパケットデータとして送られたとしても個人識別符号が「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断」されるとの認識でよろしいでしょうか。 （理由） 上記の質問事項の解釈等が明確になることは生体認証技術の適切な運用が可能となり、産業の振興にもつながると考えます。 【一般社団法人日本自動認識システム協会】	
22	対象とする事案	１．対象とする事案 質問１ （１）においては「個人データ」に関しては漏えい、滅失又は毀損を対象としているが （２）において「個人情報取扱事業者が保有する 匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号 」と「 加工方法等情報 」は漏えいのみを対象事案としている。 （２）に関しては滅失又は毀損は対象外という理解でよいか。 質問２ 「個人情報取扱事業者が保有する 匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号 」の文意が掴み難い。 つまり匿名加工情報作成の過程で元データから除去した個人情報が対象であるという理解でよいか。	質問１については、御理解のとおりです。 質問２については、御理解のとおりですが、御意見を踏まえ、本告示１．(2)を次のとおり修正します。 「個人情報取扱事業者が保有する加工方法等情報（個人情報の保護に関する法律施行規則（平成 28 年 10 月５日個人情報保護委員会規則第３号）第 20 条第１号に規定する加工方法等情報をいい、特定個人情報に係るものを除く。）の漏えい」 質問３については、一般的に現状の案で御理解頂けるものと考えます。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		質問３ 「上記（ 1）又は（2）のおそれ 」とある。 「おそれ」とは具体的にどのような事態を想定しているのか。 一般に漏えいの可能性を認識するのは外部からの指摘や不審な通信の検知が端緒であり そこから実際に調査を行ったうえで確定しない限りは民間企業は利益逸失を恐れるため、 本告知の遵守を経営層に提言しても漠然とした「おそれ」では動き得ないと思われる。 「おそれ」の具体的例示または基準を示すべきではないか。 また 具体的例示または基準が不可能であるならば 「上記（ 1）又は（2）のおそれ 」という基準自体削除すべきではないか。 【匿名】	
23	漏えい等事案が発覚した場合に講ずべき措置	・本告示２につき「個人情報取扱事業者は，漏えい等事案が発覚した場合は，次の(1)から(6)に掲げる事項について必要な措置を講ずることが望ましい。」ということは，要するに，すべてを実施することができれば素晴らしいことではあるものの，事情に応じて実施しなくとも問題がないという趣旨と理解してよいか確認されたい。あわせて本告示における「望ましい」等の表現の趣旨については通則編（1-1）と同様か回答されたい。 【金融機関における個人情報の実務研究会】	現行法及び改正後の法において、漏えい等事案に必要な措置を求める規定がないことから、法以上の対応を求めることは困難であり、「講ずることが望ましい」としています。安全管理措置に違反していると認められる場合には個人情報保護法に基づき適切な監督が行われることとなります。
24	漏えい等事案が発覚した場合に講ずべき措置	・仮に本告示における「望ましい」の表現が通則編（1-1）と同様であるとした場合，本告示違反があった場合においても直ちに法違反にはならないものと理解される。そうであれば本告示は国民の権利義務に関わる法規としての性質を有さないものであるため，本告示の法的性質は行政手続法２条８号ニの「行政指導指針」と理解して良いか確認されたい。 【金融機関における個人情報の実務研究会】	現行法及び改正後の法において、漏えい等事案に必要な措置を求める規定がないことから、法以上の対応を求めることは困難であり、「講ずることが望ましい」としています。安全管理措置に違反していると認められる場合には個人情報保護法に基づき適切な監督が行われることとなります。
25	漏えい等事案が発覚した場合に講ずべき措置	・仮に本告示の法的性質が行政手続法２条８号ニの「行政指導指針」であるとすれば，本告示の内容はあくまで任意の協力により実現されるもので（行政手続法３２条１項，２項），本告示違反自体をもって何らの不利益処分も課されないことを確認されたい。 【金融機関における個人情報の実務研究会】	現行法及び改正後の法において、漏えい等事案に必要な措置を求める規定がないことから、法以上の対応を求めることは困難であり、「講ずることが望ましい」としています。安全管理措置に違反していると認められる場合には個人情報保護法に基づき適切な監督が行われることとなります。
26	漏えい等事案が発覚した場合に講ずべき措置	・本告示２（１）につき「責任ある立場の者」とは「個人データの取扱いに関する責任者」（通則編８−３（1））のことか確認されたい。もし異なるなら，本告示２（１）の「責任ある立場の者」を定義されたい。また，同じである場合，通則編と本告示で同じ人のことについて別の呼称を用いることは混乱を招くので，平仄をあわせるか，異なる呼称を用いることが正当化される理由を説明されたい。 【金融機関における個人情報の実務研究会】	本告示2.(1)に規定する「責任ある立場の者」については、「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）」8-3.に規定する「責任ある立場の者」と同義です。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
27	漏えい等事案が発覚した場合に講ずべき措置	・本告示２（１）につき「漏えい等事案による被害が発覚時よりも拡大しないよう必要な措置」とは具体的に何か回答されたい。例えば，既に漏えい済みであれば転々流通して更に被害は拡大していくのでありその中で返還請求等を行って「被害が発覚時よりも拡大しない」ようにすることは容易ではないと思われるが，具体的に何をすればよいのかを回答されたい。１つ１つ名簿業者等を当たって転々流通する個人データを返還するよう請求する必要があるということか，確認されたい。 【金融機関における個人情報の実務研究会】	本告示2.(1)に規定する「被害が発覚時よりも拡大しないよう必要な措置」の具体的な内容については、漏えい等事案の内容・性質等の事情を勘案して個別の事例ごとに判断することとなりますが、例えば個人データの漏えいのおそれが発覚した場合に、さらなる漏えいの発生を防止するといった措置が考えられます。
28	漏えい等事案が発覚した場合に講ずべき措置	・本告示２（２）につき「事実関係の調査及び原因の究明」のための必要な措置とは具体的に何か回答されたい。例えば，第三者委員会を設置するとか，フォレンジック技術を利用する等，具体的な調査及び原因究明の手法として何が求められるのか，回答されたい。 【金融機関における個人情報の実務研究会】	本告示2.(2)に規定する「事実関係の調査及び原因の究明」の具体的な内容については、漏えい等事案の内容・性質等の事情を勘案して個別の事例ごとに判断することとなりますが、御指摘の措置も「事実関係の調査及び原因の究明」に有効と考えられます。
29	漏えい等事案が発覚した場合に講ずべき措置	・本告示２（２）につき，特定個人情報告示１．は「事実関係を調査し，番号法違反又は番号法違反のおそれが把握でた場合には，その原因の究明を行う。」としており，必ず原因の究明をしなければならないのではなく，事実関係の結果，法違反又は法違反のおそれが把握できた場合に限っている。これは，調べてみたところ法違反等はなかったとなれば，特に原因究明は不要という趣旨と解される。本告示において漏えい等事案の「おそれ」（本告示１（３））があるということで調べてみたところ，実際には，個人情報取扱事業者が保有する個人データ(特定個人情報に係るものを除く。)の漏えい，滅失又は毀損等はなかったということが判明することはあり得るということでよいか確認されたい。その上で，番号法と平仄をあわせる意味で「事実関係を調査し，漏えい等事案の存在が確認できた場合には，その原因の究明を行う。」と下線部を追加してはどうか，検討されたい。もし修正しないのであれば，その合理的理由を説明されたい。 【金融機関における個人情報の実務研究会】	本告示2.(2)に規定する「事実関係の調査及び原因の究明」の具体的な内容については、漏えい等事案の内容・性質等の事情を勘案して個別の事例ごとに判断することとなりますが、事実関係の調査の結果漏えい等事案でないことが判明した場合など、原因の究明に必要な措置が無いという場合も考えられます。一般的に現状の案で御理解頂けるものと考えます。
30	漏えい等事案が発覚した場合に講ずべき措置	・本告示２（３）につき「影響範囲の特定」というのは，誰のどのような個人情報が漏えい等しているかという点を特定するという趣旨でよいか，確認されたい。漏えい等の対象となる個人情報の特定以外に「影響範囲」があるのであれば，それは何か回答されたい。 【金融機関における個人情報の実務研究会】	御理解のとおりです。
31	漏えい等事案が発覚した場合に講ずべき措置	・本告示２（４）につき「再発防止策の検討及び実施」としてどのような行為が求められているのか回答されたい。例えば，チェック体制の強化や適切なアクセス権限の設定等が考えられるが，具体的に行うべき「再発防止策」の内容を回答されたい。 【金融機関における個人情報の実務研究会】	本告示2.(4)に規定する「再発防止策の検討及び実施」の具体的な内容については、漏えい等事案の内容・性質等の事情を勘案して個別の事例ごとに判断することとなりますが、御指摘の措置も「再発防止策の検討及び実施」に有効と考えられます。
32	漏えい等事案	・本告示２（５）につき「漏えい等事案の内容等に応じて」とは，一定の場合には影響を受ける	御理解のとおりです。本告示2.(5)に規定する「影

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
	が発覚した場合に講ずべき措置	可能性のある本人への連絡等をしなくともよいという趣旨という理解でよいか回答されたい。もしそうであれば，それはどのような場合か具体的に回答されたい。 【金融機関における個人情報の実務研究会】	響を受ける可能性のある本人への連絡等」を要しない場合については、漏えい等事案の内容・性質等の事情を勘案して個別の事例ごとに判断することとなります。なお、Q&A において、影響を受ける可能性のある本人への連絡等を要しないと考えられる場合についての考え方を示してまいります。
33	漏えい等事案が発覚した場合に講ずべき措置	・本告示２（５）につき経産省ガイドライン 2-2-3-2 では 「ただし，例えば，以下のように，本人の権利利益が侵害されておらず，今後も権利利益の侵害の可能性がない又は極めて小さいと考えられる場合には，本人への連絡を省略しても構わないものと考えられる。 ・紛失等した個人データを，第三者に見られることなく，速やかに回収した場合 ・高度な暗号化等の秘匿化が施されている場合(ただし，(オ)に定める報告の際，高度な暗号化等の秘匿化として施していた措置内容を具体的に報告すること。) ・漏えい等をした事業者以外では，特定の個人を識別することができない場合(事業者が所有する個人データと照合することによって，はじめて個人データとなる場合。ただし，(オ)に定める報告の際，漏えい等をした事業者以外では特定の個人を識別することができないものと判断できる措置内容を具体的に報告すること。)」 とされているが，本告示の下において，上記の各場合においてもなお本人への連絡等をしなければならないのか確認されたい。もししなければならないのであれば，なぜ経産省ガイドラインと異なるのか理由を説明されたい。もししなくてよいのであれば，その旨を本告示において明示されたい。 【金融機関における個人情報の実務研究会】	本告示 2.(5)に規定する「影響を受ける可能性のある本人への連絡等」については、「漏えい等事案の内容等に応じて」必要な措置を講ずることが望ましいと規定しているとおり、漏えい等事案の内容・性質等の事情を勘案して個別の事例ごとに判断することとなります。なお、Q&A において、影響を受ける可能性のある本人への連絡等を要しないと考えられる場合についての考え方を示してまいります。
34	漏えい等事案が発覚した場合に講ずべき措置	・本告示２（５）につき，本人に対して「連絡」をする代わりに「本人が容易に知り得る状態に置く」ことでもよいという理解でよいか確認されたい。その上で，この「容易に知り得る」の意味は通則編 3-4-2-1*2 の「「本人が容易に知り得る状態」とは，事業所の窓口等への書面の掲示・備付けやホームページへの掲載その他の継続的方法により，本人が知ろうとすれば，時間的にも，その手段においても，簡単に知ることができる状態をいい，事業の性質及び個人情報の取扱状況に応じ，本人が確実に認識できる適切かつ合理的な方法によらなければならない(規則第 7 条第 1 項第 2 号)。 【本人が容易に知り得る状態に該当する事例】 事 例　1)本人が閲覧することが合理的に予測される個人情報取扱事業者のホームページにおいて，本人が分かりやすい場所(例:ホームページのトップページから 1 回程度の操作で到達できる場所等)に法に定められた事項を分かりやすく継続的に掲載する場合 事例 2)本人が来訪することが合理的に予測される事務所の窓口等への掲示，備付け等が継続的	いずれも御理解のとおりです。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		に行われている場合 事例 3)本人に頒布されている定期刊行物への定期的掲載を行っている場合 事例 4)電子商取引において，商品を紹介するホームページにリンク先を継続 的に表示する場合」が適用されるということでよいか，回答されたい。 【金融機関における個人情報の実務研究会】	
35	漏えい等事案が発覚した場合に講ずべき措置	・本告示２（６）につき「漏えい等事案の内容等に応じて」とは，一定の場合には事実関係及び再発防止策等の公表をしなくともよいという趣旨という理解でよいか回答されたい。もしそうであれば，それがどのような場合か具体的に回答されたい。 【金融機関における個人情報の実務研究会】	御理解のとおりです。本告示 2.(6)に規定する「事実関係及び再発防止策等の公表」を要しない場合については、漏えい等事案の内容・性質等の事情を勘案して個別の事例ごとに判断することとなります。なお、Q&A において、事実関係及び再発防止策の公表を要しないと考えられる場合についての考え方を示してまいります。
36	漏えい等事案が発覚した場合に講ずべき措置	・本告示２（６）につき，経産省ガイドライン 2-2-3-2 では「ただし，例えば，以下のように，二次被害の防止の観点から公表の必要性がない場合には，事実関係等の公表を省略しても構わないものと考えられる。なお，そのような場合も，類似事案の発生回避の観点から，同業種間等で，当該事案に関する情報が共有されることが望ましい。 ・影響を受ける可能性のある本人すべてに連絡がついた場合 ・紛失等した個人データを，第三者に見られることなく，速やかに回収した場合 ・高度な暗号化等の秘匿化が施されている場合(ただし，(オ)に定める報告の際，高度な暗号化等の秘匿化として施していた措置内容を具体的に報告すること。) ・漏えい等をした事業者以外では，特定の個人を識別することができない場合(事業者が所有する個人データと照合することによって，はじめて個人データとなる場合。ただし，(オ)に定める報告の際，漏えい等をした事業者以外では特定の個人を識別することができないものと判断できる措置内容を具体的に報告すること。)」とされているが，本告示の下において，上記のような場合においてもなお事実関係及び再発防止策等の公表をしなければならないのか確認されたい。もし，しなければならないのであれば，なぜ経産省ガイドラインと異なるのか理由を説明されたい。もししなくてよいのであれば，その旨を本告示において明示されたい。 【金融機関における個人情報の実務研究会】	本告示 2.(6)に規定する「事実関係及び再発防止策等の公表」については、「漏えい等事案の内容等に応じて」必要な措置を講ずることが望ましいと規定しているとおり、漏えい等事案の内容・性質等の事情を勘案して個別の事例ごとに判断することとなります。なお、Q&A において、事実関係及び再発防止策の公表を要しないと考えられる場合についての考え方を示してまいります。
37	漏えい等事案が発覚した場合に講ずべき措置	（該当箇所） ２ページ、　「２．漏えい等事案が発覚した場合に講ずべき措置」 （意見） 事業者がそれぞれの措置を「講ずるか否か」を検討する際に判断材料となるような具体例を示すと効果的ではないでしょうか。また、将来的に、こうした具体例をＱ＆Ａのような形で公表されるお考えはあるでしょうか。	影響を受ける可能性のある本人への連絡等並びに事実関係及び再発防止策等の公表を要しないと考えられる場合について、Q&A において考え方を示してまいります。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		（理由） 「3.(2)　委員会への報告を要しない場合」には複数具体例が示されていますが、こちらにはありません。また、特に、「（５）本人への連絡」や「（６）公表」については、個人情報取扱事業者と消費者の間に認識の差があり、後にトラブルになる事例が多いため、指標となる事例を示す必要があると考えます。なお、現行の経済産業省ガイドラインでは、事例が示されており、事業者の判断に役立っています。 【一般財団法人日本情報経済社会推進協会】	
38	漏えい等事案が発覚した場合に講ずべき措置	（該当箇所） ２ページ、　「２．漏えい等事案が発覚した場合に講ずべき措置」 （意見） 「次の(1)から(6)に掲げる事業について必要な措置を講ずることが望ましい」とありますが、「望ましい」に止めるのではなく、「原則として講ずる」のが適しているのではないでしょうか。 （理由） 漏えい等発生した事案の影響度に依るとは思いますが、いずれも、本来、原則として講ずべき措置であるように思われます。個人情報保護委員会ガイドライン（通則編）「3-3-2　安全管理措置（法 20 条関係）」では、漏えい等の発生防止のために「具体的に講じなければならない措置や当該項目を実践するための手法例等･･･」と記載されており、それとのバランスにも考慮すべきと思います。 【一般財団法人日本情報経済社会推進協会】	現行法及び改正後の法において、漏えい等事案に必要な措置を求める規定がないことから、法以上の対応を求めることは困難であり、「講ずることが望ましい」としています。
39	漏えい等事案が発覚した場合に講ずべき措置	漏えい等事案が発覚した場合に構ずべき措置として(1)から(6)の事項が示されましたが、そもそも「漏えい等事案が発覚した場合の(1)から(6)への対応の手順」を整備していなければ、「(1)から(6)の措置」を講じることは難しいでしょう。 この項の本文は「個人情報取扱事業者は、漏えい等事案が発覚した場合は、次の（1）から（6）に掲げる事項について必要な措置を講ずることが望ましい。」となっていますが「個人情報取扱事業者は、漏えい等事案が発覚した場合に、次の（1）から（6）に掲げる事項について必要な措置を講じられるよう、その手順を整備することが望ましい。」とした方が有効なものになるのではないでしょうか？ 例えば、「（6）事実関係及び再発防止策等の公表」では「漏えい等事案の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、事実関係及び再発防止策等について、速やかに公表する。」となっていても、「二次被害の防止、類似事案の発生防止等の観点から」という箇所が重要なところで、インターネットを介して情報が漏えいした場合などは、その情報を完全に消去できた上で公表しないと被害が拡大してしまいます。 単に「必要な措置を講ずる」ではなく「必要な措置を講じられるよう、その手順を整備する」と言った方が実効性が高まると考えますが、今回示された「案」の中からそこまでを読み解き、現状の案で理解しないといけないものなのでしょうか。	一般的に現状の案で御理解頂けるものと考えます。なお、御指摘の事実関係及び再発防止策の公表については、Q&A において考え方を示してまいります。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		【改正個人情報保護法　消費者志向で考える事業者ガイドライン研究会】	
40	漏えい等事案が発覚した場合に講ずべき措置	漏えい等事案が発覚した場合に構ずべき措置として(1)から(6)の事項が示されましたが、そもそも「漏えい等事案が発覚した場合の(1)から(6)への対応の手順」を整備していなければ、「(1)から(6)の措置」を講じることは難しいでしょう。 この項の本文は「個人情報取扱事業者は、漏えい等事案が発覚した場合は、次の（1）から（6）に掲げる事項について必要な措置を講ずることが望ましい。」となっていますが「個人情報取扱事業者は、漏えい等事案が発覚した場合に、次の（1）から（6）に掲げる事項について必要な措置を講じられるよう、その手順を整備することが望ましい。」とした方が有効なものになるのではないでしょうか？ 例えば、「（6）事実関係及び再発防止策等の公表」では「漏えい等事案の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、事実関係及び再発防止策等について、速やかに公表する。」となっていても、「二次被害の防止、類似事案の発生防止等の観点から」という箇所が重要なところで、インターネットを介して情報が漏えいした場合などは、その情報を完全に消去できた上で公表しないと被害が拡大してしまいます。 単に「必要な措置を講ずる」ではなく「必要な措置を講じられるよう、その手順を整備する」と言った方が実効性が高まると考えますが、今回示された「案」の中からそこまでを読み解き、現状の案で理解しないといけないものなのでしょうか。 【公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会】	一般的に現状の案で御理解頂けるものと考えます。なお、御指摘の事実関係及び再発防止策の公表については、Q&A において考え方を示してまいります。
41	漏えい等事案が発覚した場合に講ずべき措置	（該当箇所）　２頁 2.(5)「影響を受ける可能性のある本人への連絡等」 2.(6)「事実関係及び再発防止策等の公表」 __の文中２箇所 （意見） 文中の「漏えい等事案の内容等に応じて」を「漏えい等事案の内容を判断し、想定される影響度等に応じて」に変更する。 （理由） 変更箇所を具体的に、「等」の一例として「想定される影響度」と追記することにより、漏洩事案対応の一般則を盛り込むことが出来ると考えます。 【日本オラクル株式会社】	一般的に現状の案で御理解頂けるものと考えます。なお、影響を受ける可能性のある本人への連絡等並びに事実関係及び再発防止策等の公表を要しないと考えられる場合について、Q&A において考え方を示してまいります。
42	漏えい等事案が発覚した場合に講ずべき措置	「２．漏えい等事案が発覚 した場合に講ずべき措置」で６項目の事項が挙げられているが、その前提として「コンプライアンスの遵守」を追記したほうがよい。 理由） 　データ漏えいの発覚の契機が、反社会的勢力からの連絡によるもので、その内容が「データの買取	御指摘の点は、本告示が規定する漏えい等事案への対応に限らず、事業の遂行全般に当然に妥当する事項であり、本告示に特別の規定を置くまでもなく、一般的に現状の案で御理解頂けるものと考えます。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		り、破棄」に対する対価の暗黙的な金銭要求等の場合がある。 「被害拡大防止」を最優先とするあまり反社会的勢力への資金提供や裏取引をおこなうことを防止することが重要である。 反社会的勢力による不当要求には一切応じず、毅然として法的対応行うためにもこのような場合は警察・暴力追放運動推進センター・弁護士等の 外部専門機関と連携し、組織的かつ適正に対応する必要がある。 【個人】	
43	漏えい等事案が発覚した場合に講ずべき措置	漏えい等事案が発覚した場合に講ずべき措置における、「個人情報取扱事業者は、漏えい等事案が発覚した場合は、次の（1）から（6）に掲げる事項について必要な措置を講ずることが望ましい。」について。 「必要な措置を講ずることが望ましい」という弱い表現では、例えば漏えい等事案の隠蔽を意図する個人情報取扱事業者などにより、必要な措置を講じない抜け穴とされるおそれがあるため、「必要な措置を原則として行う」などのより強い表現とすべきではないか。 【個人】	現行法及び改正後の法において、漏えい等事案に必要な措置を求める規定がないことから、法以上の対応を求めることは困難であり、「講ずることが望ましい」としています。
44	漏えい等事案が発覚した場合に講ずべき措置	２．漏えい等事案が発覚した場合に講ずべき措置の（6）事実関係及び再発防止対策等の公表では、公表を省略できる事例が記載されていない。現行「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」の 30 ページ「（カ）事実関係、再発防止策等の公表」では、「例えば、以下のように、二次被害の防止の観点から公表の必要性がない場合には事実関係等の公表を省略しても構わないものと考えられる」とあり、「影響を受ける可能性のある本人すべてに連絡がついた場合」など四つの場合が記載されている。本人すべてに連絡がついた場合以外は、３．個人情報保護委員会等への報告の（2）報告を要しない場合に記載されているが、公表と報告は異なるのだから、（6）事実関係及び再発防止策等の公表でも記述するほうがよいのではないか。本人すべてに連絡がついた場合も公表省略の妥当性があると思われるので、復活させるべきである。 【個人】	影響を受ける可能性のある本人への連絡等並びに事実関係及び再発防止策等の公表については、「漏えい等事案の内容等に応じて」としているところですが、これらの措置を要しないと考えられる場合について、Q&A において考え方を示してまいります。
45	漏えい等事案が発覚した場合に講ずべき措置	（該当箇所） 2 ページ 11 行～16 行 （意見） 2.漏えい等事案が発覚した場合に講ずべき措置(5)、(6)について、漏えい等事案の内容等に応じてと条件付け、とるべき措置が記載されています。漏えい等事案の内容等に応じて対応する事例として次のように考えてよいのでしょうか。 ・(5)については、「影響を受ける可能性のある本人への連絡等」を求めないものとして、P.3（※3）の事例全てが該当すると考えていいのでしょうか？ ・(6)については、「事実関係及び再発防止策等の公表」を求めないものとして、影響を受ける可能性	影響を受ける可能性のある本人への連絡等、事実関係及び再発防止策等の公表並びに個人情報保護委員会等への報告のいずれも、性質を異にすると考えます。このため、個人情報保護委員会等への報告を要しない場合と、①影響を受ける可能性のある本人への連絡等又は②事実関係及び再発防止策等の公表を要しない場合はそれぞれ要件を異にするものと考えられることから、①及び②のそれぞれについて Q&A において考え方を示してまいります。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		のある本人すべてに連絡がついた場合及びP.3（※3）の事例全てが該当すると考えていいのでしょうか？ また、事例として※３を引用し明記していただけないでしょうか。 （理由） 漏えい等事案の内容等に応じてと規定されていることについて、典型的な事例が記載されていないので、受け取り方にばらつきが生じる可能性があります。 【匿名】	
46	個人情報保護委員会等への報告	・本告示３（１）では報告先は記載されても「報告の方法」，例えば書面なのか，メールなのか，どのような書式なのか等が記載されていない。どのような書式でどのように報告すべきかを回答されたい。 【金融機関における個人情報の実務研究会】	参考となる報告書の様式を、個人情報保護委員会のホームページに掲載する予定です。
47	個人情報保護委員会等への報告	・本告示３の「漏えい等事案が発覚した場合」とは本告示２（１）の前ということか，それとも（６）の後ということか，本告示２（１）から（６）の流れのどこに個人情報保護委員会への報告が位置づけられるのか回答されたい。 【金融機関における個人情報の実務研究会】	漏えい等事案の内容・性質等の事情によりますが、個人情報保護委員会等への報告については、「速やかに」行うことが望ましいと考えられます。
48	個人情報保護委員会等への報告	・本告示３（１）は，原則個人情報保護委員会，例外は報告徴収及び立入検査が事業所管大臣に委任されている分野と読めるが，この原則・例外の書き方は，「事業者における特定個人情報告示２（１）アとは逆である。なぜ番号法と個人情報保護法において対応が逆なのか，その合理的な理由を説明されたい。合理的理由がなければ，平仄をあわせるべきであろう。 【金融機関における個人情報の実務研究会】	改正後の法においては、個人情報取扱事業者に対する監督に係る権限が個人情報保護委員会に一元化されるため、御指摘のような規定としています。
49	個人情報保護委員会等への報告	・本告示３（２）①につき，「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合」には，通則編及び本告示における「漏えい」に該当しないと理解してよいか，回答されたい。 【金融機関における個人情報の実務研究会】	「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合」とは、漏えい等事案に該当するものの、個人情報保護委員会事務局等への報告を要しないと考えられる場合のことです。
50	個人情報保護委員会等への報告	・本告示３（２）の報告を要しない場合として事実関係の調査を了し，再発防止策を決定している場合を含める必要はないか検討されたい。もし不要であれば，その理由，特に，特定個人情報告示２（２）③との平仄の観点からなぜ含めないことが正当化されるのかについての合理的理由を説明されたい。 【金融機関における個人情報の実務研究会】	事実関係の調査を了し、再発防止策を決定している場合であっても、漏えい等事案の社会的な影響の度合い等に照らして個人情報保護委員会等に情報提供するよう努めるべき場合はあり得ますので、御指摘の事由については、報告を要しない場合として規定していません。
51	個人情報保護委員会等への報告	・本告示３（２）の報告を要しない場合として影響を受ける可能性のある本人全てに連絡した場合(本人への連絡が困難な場合には，本人が容易に知り得る状態に置くことを含む。)を含める必要はないか検討されたい。もし不要であれば，その理由，特に，特定個人情報告示２（２）①との平仄の観	影響を受ける可能性のある本人全てに連絡した場合（本人への連絡が困難な場合には、本人が容易に知り得る状態に置くことを含む。）であっても、漏え

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		点からなぜ含めないことが正当化されるのかについての合理的理由を説明されたい。 【金融機関における個人情報の実務研究会】	い等事案の社会的な影響の度合い等に照らして個人情報保護委員会等に情報提供するよう努めるべき場合はあり得ますので、御指摘の事由については、報告を要しない場合として規定していません。
52	個人情報保護委員会等への報告	・本告示３（２）の報告を要しない場合として「特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則」(平成 27 年特定個人情報保護委員会規則第５号。以下「規則」という。)第 2 条に規定する特定個人情報ファイルに記録された特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態(以下「重大事態」という。)に該当しない場合を含める必要はないか検討されたい。もし不要であれば，その理由，特に特定個人情報告示２（２）④との平仄の観点からなぜ含めないことが正当化されるのかについての合理的理由を説明されたい。 【金融機関における個人情報の実務研究会】	御指摘の重大事態は、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年 5 月 31 日法律第 27 号）第 28 条の 4 の規定に基づき定められるものであり、本告示が対象とする特定個人情報以外の個人情報の漏えい等の事案に適用されるものではないため、本告示において規定する必要がないものと考えます。
53	個人情報保護委員会等への報告	・本告示３（２）①につき，もし「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合」でも通則編及び本告示における「漏えい」に該当すると解釈される場合，「漏えい等事案を生じた事業者以外の者は，漏えい等事案に係る個人データ又は加工方法等情報によって特定の個人を識別することができない」場合であっても「漏えい」に該当するということになるが，このような場合は，個人情報取扱事業者にとっては個人データであっても第三者，つまり漏えいの相手方にとっては個人データではない以上，漏えいの定義に該当しないのではないか，確認されたい。もしそれでも漏えいの定義に該当するというのであれば，その理由を回答されたい。 【金融機関における個人情報の実務研究会】	御意見は、本意見募集の対象外と考えます。漏えい、滅失若しくは毀損又はこれらのおそれに係る情報が個人データ又は加工方法等情報に該当するか否かは、当該情報を保有していた個人情報取扱事業者を基準として判断されます。
54	個人情報保護委員会等への報告	・本告示３（２）①につき，何が「高度」な暗号化か回答されたい。例えば，この暗号化技術を使えば「高度」で，そうでなければ「高度」ではないとか，特定の基準・標準を満たしたり認証を受けていれば「高度」であるといった具体的な基準を明らかにされたい。（それとも，個人情報取扱事業者として主観的にないしは何らかの根拠をもって「高度」と考えていればそれだけでこの「高度」な暗号化に該当するということであればその旨回答されたい。） 【金融機関における個人情報の実務研究会】	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033 等に掲載されている暗

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
			号技術が用いられ、それが適切に実装されていることが考えられます。 　また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。
55	個人情報保護委員会等への報告	・本告示３（２）①につき，「第三者に閲覧されないうちに全てを回収した」というのは，合理的にみて第三者が閲覧するだけの時間的余裕がない短期間のうちに回収できた場合にはこれに該当することを確認されたい。（「閲覧されない」ことの証明はいわゆる「悪魔の証明」であって，速やかに回収された結果合理的にみて第三者が閲覧するだけの時間的余裕がない場合等，合理的に考えて「閲覧されないうち」と認定できる場合がこの要件に該当することを認めてもらえないと，この要件に該当する事例が事実上存在しなくなるため。） 【金融機関における個人情報の実務研究会】	本告示3.(2)①に規定する「第三者に閲覧されないうちに全てを回収した場合」については、御指摘のような回収までに要した時間等の事情を勘案して個別の事例ごとに判断することとなりますが、例えば、誤ってウェブサイトに掲載され、誰もが閲覧可能な状態に置かれたものの、掲載を停止するまでの間に誰にも閲覧されていないことがアクセスログから明らかである場合などが考えられます。
56	個人情報保護委員会等への報告	・本告示３（２）①につき，「毀損」又は「滅失」が発生し，「漏えい」が発生していない場合は「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合」であるといってよいか確認されたい。もし、「毀損」又は「滅失」が発生し，「漏えい」が発生していない場合のうち，「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合」とはいえない場合があるというのであれば，それがどのような場合か具体的に回答されたい。 【金融機関における個人情報の実務研究会】	御理解のとおりです。
57	個人情報保護委員会等への報告	・本告示３（２）①につき，「漏えい等事案に係る個人データ又は加工方法等情報によって特定の個人を識別することが漏えい等事案を生じた事業者以外ではできない場合」だけれども「漏えい等事案に係る個人データ又は加工方法等情報のみで，本人に被害が生じるおそれのある情報」が漏えいした場合というのはどのような場合が想定されるのか，具体的に回答されたい。存在しないのであれば削除されたい。（そもそも第三者にとって個人を識別できないなら「本人」に被害は生じないし，本人に被害が生じるなら，第三者にとって個人を識別できることから，このような場合は存在しないのではないかという趣旨で質問している。） 【金融機関における個人情報の実務研究会】	漏えい等事案に係る個人データ又は加工方法等情報の内容や性質等を勘案して個別の事例ごとに判断することとなりますが、例えば、携帯電話番号のようにそれが利用された場合に本人が見ず知らずの者から不測の接触を受けるなど、その情報のみで本人に被害が生じるおそれのある情報が該当すると考えられます。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
58	個人情報保護委員会等への報告	・本告示３（２）①につき，「個人データ又は加工方法等情報の滅失又は毀損にとどまり，第三者が漏えい等事案に係る個人データ又は加工方法等情報を閲覧することが合理的に予測できない場合」というのは，滅失・毀損であれば通常「第三者が漏えい等事案に係る個人データ又は加工方法等情報を閲覧することが合理的に予測できない場合」と言ってよいか回答されたい。例えば，ある個人データが滅失したが，その原因が不明で，ハードの問題かもしれないしソフトの問題かもしれないし，内部者の犯行かもしれないし，外部者の犯行かもしれないという場合において，「個人データ又は加工方法等情報の滅失又は毀損にとどまり，第三者が漏えい等事案に係る個人データ又は加工方法等情報を閲覧することが合理的に予測できない場合」といえるか回答されたい。 【金融機関における個人情報の実務研究会】	御理解のとおりです。
59	個人情報保護委員会等への報告	・本告示３（２）②につき，そもそもFAX，メール，荷物の「宛名及び送信者名」というのは，散在情報であり個人データではないから，「FAX 若しくはメールの誤送信，又は荷物の誤配等のうち，宛名及び送信者名以外に個人データ又は加工方法等情報が含まれていない場合」は，本告示３（２）②によって報告が不要になるのではなく，そもそも本告示のいう漏えい等事案（本告示１，特に１（１）参照）ではないのではないか，確認されたい。もし漏えい等事案になるというのであれば，なぜデータベース化されていない単なるFAX，メール，荷物の「宛名及び送信者名」が誤って第三者に見られたことが漏えい等事案に該当するのかを説明されたい。 【金融機関における個人情報の実務研究会】	FAX、メール、荷物等の宛先欄又は送付元欄に記載された情報は、それが個人情報データベース等を構成する情報から出力されたものであれば、個人データに該当するものと考えられます。
60	個人情報保護委員会等への報告	・本告示３（２）②につき，個人データベースから出力した紙媒体の情報を発送したが，個人データベースの住所情報が間違っていたため，誤配になる場合（その他の情報は正確とする。）は，「FAX若しくはメールの誤送信，又は荷物の誤配等のうち，宛名及び送信者名以外に個人データ又は加工方法等情報が含まれていない場合」に該当するのか，回答されたい。 【金融機関における個人情報の実務研究会】	御指摘の趣旨が必ずしも明らかでありませんが、御指摘の「紙媒体の情報」が宛名及び送信者名のみを構成するものであり、その他に個人データ又は加工方法等情報が含まれていないものが誤配となったという場合であれば、本告示3.(2)②に規定する「FAX若しくはメールの誤送信、又は荷物の誤配等のうち軽微なものの場合」に該当するものと考えられます。
61	個人情報保護委員会等への報告	・本告示３（２）②につき「FAX若しくはメールの誤送信，又は荷物の誤配等のうち，宛名及び送信者名以外に個人データ又は加工方法等情報が含まれていない場合」とあるが，例えば荷物の中（外部から見ることができないところ）に個人データが含まれていたが，誤配された相手が荷物を開封しなかったので，相手は個人データを見ていないという場合には，「FAX 若しくはメールの誤送信，又は荷物の誤配等のうち，宛名及び送信者名以外に個人データ又は加工方法等情報が含まれていない場合」に該当するということでいいか，確認されたい。 【金融機関における個人情報の実務研究会】	御指摘の場合において、誤配された相手その他の第三者によって荷物が開封されることなく回収された場合には、本告示3.(2)①に規定する「漏えい等事案に係る個人データ又は加工方法等情報を第三者に閲覧されないうちに全てを回収した場合」に該当するものと考えられます。
62	個人情報保護委員会等への	意見① （該当箇所）	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
	報告	２ページ・１７行目以降記載の、３．個人情報保護委員会等への報告に関し、 （意見） Ｐ３の（2）報告を要しない場合 次の①又は②のいずれかに該当する場合は、報告を要しない（※2）。 （※2） この場合も、事実関係の調査及び原因の究明並びに再発防止策の検討及び実施をはじめとする上記 2.の各対応を実施することが、同様に望ましい。 ①実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合（※3） ・漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合 に関し、 過去の各省庁や貴委員会と弊コンソーシアムとの意見交換等では、高度な暗号化とは、主として政府推奨暗号を意図しているが、実際には現場で判断すべき内容でその時点で最善の暗号を用いること。しかも、暗号鍵管理も含めた総合的な安全管理を意図している。抽象的な表現であるが暗号化だけが対策ではない。との認識で良いか。 （理由） 現場での対処には、例示中の「高度な暗号化等」が実際のところ何を示すのかが判然としないままだと適切な安全管理措置の検討・実施自体に支障を来すから。 【秘密分散法コンソーシアム】	暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。
63	個人情報保護委員会等への報告	意見② （該当箇所） ２ページ・１７行目以降記載の、３．個人情報保護委員会等への報告に関し、 前述の意見①と同じ部分です。 （意見） 過去の各省庁や貴委員会と弊コンソーシアムとの意見交換等では、高度な暗号化等の「等」には、暗号以外の技術で且つ、高度な暗号化と同等、またはそれ以上と判断できる技術で、現場で利活用できるものが対象として考えられる。との認識が示されているが、これは現場が、暗号化以外でも有用と考えられる技術等を適切に選択できるようにできるよう意図された記述と考えて良いか。また、そうした際のポイントは、万が一のデータ流出等の際に、その流出等したデータそのものから、現場の関与が及ばない範囲で、見読される可能性が実質的に無いレベルの秘匿化という意味と考えてよろしい	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となる

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		か。更に、流出等したデータから、仮に全体でなくても一部が復号・解読され、その他照会できるインターネット上等の情報と照合し、本人特定できてしまうことができれば当然閲覧されてしまう可能性も出てしまうので対象とはならない。と考えるが、よろしいか。 （理由） 現場での対処には、例示中の「高度な暗号化等」が実際のところ何を示すのか、またどのような意図の元に存在する記述なのかが判然としないままだと、適切な安全管理措置の検討・実施自体に支障を来すから。 【秘密分散法コンソーシアム】	ような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。
64	個人情報保護委員会等への報告	意見③ （該当箇所） ２ページ・１７行目以降記載の、３．個人情報保護委員会等への報告に関し、 前述の意見①、②と同じ部分です。 （意見） 政府推奨暗号リストの策定に携わるクリプトレックは、漏えい後も個人情報保護法の法令の要求する長期間の安全管理措置に対し、解読可能性が無いと保証してくれているうえでの当パブコメ内容ではないと考えるが、従前の各省主務大臣等への報告内容に準じた内容で、既知の各省ガイドライン記載事項（経済産業省等のガイドライン等）の、報告を要しない例を参考としたものとの認識でよろしいか。また、高度な暗号化等の「等」に該当する技術等の中の一つに、①政府機関の情報セキュリティ対策のための統一基準(2005 年 12 月版(全体版初版)解説書や②政府機関の情報セキュリティ対策のための統一技術基準（平成 24 年度版）　解説書、③平成 26 年版府省庁対策基準策定のためのガイドライン等に、暗号とは異なるセキュリティ技術として秘密分散技術が具体的な利用シーンと共に記載公表され、要機密情報や要安定情報への安全確保の手法として記載され、公共等でも採用されてきたが、その対象となる適切な実装がなされた秘密分散技術のうち、適切な当該技術等の利活用により法令の定義項から除外される特性を持つ秘密分散技術の適切な利活用が、高度な暗号化等の「等」のひとつに入ると我々コンソーシアムは認識しているが、認識としてよろしいか。 ①（http://www.nisc.go.jp/active/general/pdf/k303-052c.pdf） ②（http://www.nisc.go.jp/active/general/pdf/K305-111C.pdf） ③（http://www.nisc.go.jp/active/general/pdf/guide26.pdf）	クリプトレックについては、御理解のとおりです。 実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		（理由） 現場での対処の現実解を得るためには、例示の中の「高度な暗号化等」の「等」に選択可能な技術が実在するかを示さなければ、適切な安全管理措置の検討・実施自体に支障を来すから。 【秘密分散法コンソーシアム】	鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。 なお、「高度な暗号化等の秘匿化がされている場合」の考え方を Q&A で示してまいりますが、Q&A の内容は技術の進展等を踏まえ見直される場合がありますので、最新の Q&A を御参照下さい。
65	個人情報保護委員会等への報告	意見④ （該当箇所） ２ページ・１７行目以降記載の、３．個人情報保護委員会等への報告に関し、 前述の意見①、②、③と同じ部分です。 （意見） 個人情報保護委員会として、漏えい後も個人情報保護法の法令の要求する長期間の安全管理措置に対し、解読可能性が無いと保証してくれているうえでの当パブコメ内容ではないと考えるがよろしいか。また、貴委員会としては本来個人データ等の漏えい等が発生しないよう注意喚起しており、当パブコメの位置づけは、万が一の流出等の事故発生時を想定したもので、流出等が発生した場合に外部の他の組織等で対象となる個人情報等が閲覧できないよう、特定の個人が識別されないような秘匿化（この場合の秘匿化は、暗号化以外であっても前述のように「等」に該当するものであれば良い）が為されていれば、実質的に漏えいしていない。と言えるのではないか。という参考を例示したものであると認識しており、最終的判断は現場が行うこととなると考えているが、よろしいか。 （理由） 現場での対処の現実解を得るためには、例示の中の「高度な暗号化等」の「等」に選択可能な技術が実在するかを示さなければ、適切な安全管理措置の検討・実施自体に支障を来すから。 【秘密分散法コンソーシアム】	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
			満たすことが必要と解されます。 なお、「高度な暗号化等の秘匿化」に該当するか否かは、漏えい等事案が生じた時点の技術水準に照らして客観的に判断されます。また、「高度な暗号化等の秘匿化がされている場合」の考え方を Q&A で示してまいりますが、Q&A の内容は技術の進展等を踏まえ見直される場合がありますので、最新の Q&A を御参照下さい。
66	個人情報保護委員会等への報告	意見⑤ （該当箇所） ２ページ・１７行目以降記載の、３．個人情報保護委員会等への報告に関し、 前述の意見①、②、③、④と同じ部分です。 （意見） 事業者等現場の判断で、高度な暗号化等を実施していたとして、当パブコメ記載内容に従い報告しないでいて、実は本来の管理組織以外の外部で見読・閲覧できてしまっていて被害が拡大していた場合、個人情報保護委員会はどのような対処を行い、どのような罰則が適用されるのかに関しては、現時点の法律上の委員会報告は、努力義務であり、（明らかな重大事態の場合は、異なると思いますが（XXXXXXXXXXXXX））先ず、法律上の権限行使ではなく、任意の報告を行い、次に、その内容等を貴委員会等で確認し、その後法令に従い判断するものと認識しており、「実質的に漏えいしていない」と言えるかどうかが大きな判断基準となると推測するが、現場実務場面においては、やはり現場が判断することとなると考えているが、よろしいか。 （理由） 一般論として、公的な組織から公表される資料中の注目される記述は、その部分だけが「一人歩き」しやすい性質を持つ。今回の案では、「報告を要しない場合」の記述が相当すると考える。最終的な安全管理義務を負うべきは誰なのかを、再度注意喚起し、適切な安全管理措置の検討・実施を現場に認識してもらう必要があると考えるから。 【秘密分散法コンソーシアム】	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストや ISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。 なお、「高度な暗号化等の秘匿化」に該当するか否

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
			かは、漏えい等事案が生じた時点の技術水準に照らして客観的に判断されます。
67	個人情報保護委員会等への報告	意見⑥ （該当箇所） ２ページ・１７行目以降記載の、３．個人情報保護委員会等への報告 Ｐ３の、①実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合（※3） の記載事項に関し、 （意見） ・漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合 に関し、 「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）」の個人情報定義項に関する解説の記述部には、「～暗号化等によって秘匿化されているかどうかを問わない」とある。当パブコメが対象としている個人データが個人情報であることは疑いようが無いことと認識しているがよろしいか。また、近年の事件では、当事者が気づかないうちに暗号鍵やＩＤ／パスワード等も同時に流出することや、効果的な暗号に対する攻撃手法を敢えて公表しない攻撃者が存在することも否定できない。更に、個人データ流出後も個人情報保護法の要求する長期間の安全管理義務対象期間中の安全性が暗号のみで確約されているとは考えられず、高度な暗号化等の「等」に該当する技術の選択肢が市場顕在化することは大きな社会的意義があると考えるが、よろしいか。更に、既存暗号技術と高度な暗号化等の「等」に該当する技術等を組み合わせて流出後の解読等のリスク最小化の措置を実施することは、理論的には大学の理工系でも履修していると思われる、複数の異なる種類のセキュリティ技術等を組み合わせて使用し、より安全性を高める「多重化」に相当し、具体的には①政府機関の情報セキュリティ対策のための統一基準(2005 年 12 月版(全体版初版)解説書や②平成 26 年版府省庁対策基準策定のためのガイドライン等にも記載される手法であり、実質的に外部に漏えいしていないと考えられる現実的な安全管理措置の一つと考えるが、よろしいか。 ①（http://www.nisc.go.jp/active/general/pdf/k303-052c.pdf） ②（http://www.nisc.go.jp/active/general/pdf/guide26.pdf） （理由） 実質的に情報漏えいしていない。と判断できる対策を考えるとき、対象となる情報の性質上長期間の安全性確保を無視できない。そこで既存技術だけに依存することでのリスク顕在化を未然防止すべく、新たな技術等も組み合わせて有効活用し、既存技術が危殆化等したとしてもなお、安全性が損なわれないような対策も具体化する必要があると考えるから。 【秘密分散法コンソーシアム】	「高度な暗号化等の秘匿化がされている」情報が個人情報であるという御指摘については、御理解のとおりです。 「高度な暗号化等の秘匿化がされている場合」という規定の仕方に対する御意見は、賛同の御意見として承ります。 「高度な暗号化等の秘匿化がされている場合」に該当するか否かは、漏えい等事案が生じた時点の技術水準に照らして客観的に判断されます。なお、「高度な暗号化等の秘匿化がされている場合」の考え方を Q&A で示してまいりますが、Q&A の内容は技術の進展等を踏まえ見直される場合がありますので、最新の Q&A を御参照下さい。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
68	個人情報保護委員会等への報告	意見⑦ （該当箇所） ２ページ・１７行目以降記載の、３．個人情報保護委員会等への報告 Ｐ３の、①実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合（※3） の記載事項に関し、 （意見） ・漏えい等事案に係る個人データ又は加工方法等情報を第三者に閲覧されないうちに全てを回収した場合 に関し、 「全て」の対象が流出後の不正コピー等も範疇に入るとすれば、事実上不可能な要件と考える。仮に前述の不正コピー等が範疇外だとして、例えば物理的な封書でも電子データの場合でも、そもそも一般論として現時点の技術では一切外部に閲覧されないで全てを回収しきった。ということを証明すること自体ができないと弊コンソーシアムとして考えるが、いかがか？ （理由） 現時点では、流出してしまった個人データを第三者に閲覧されずに全て回収したことの確証を得られる仕組みが存在しないと考えられるから。 【秘密分散法コンソーシアム】	本告示3.(2)①に規定する「第三者に閲覧されないうちに全てを回収した場合」については、回収までに要した時間等の事情を勘案して個別の事例ごとに判断することとなりますが、例えば、誤ってウェブサイトに掲載され、誰もが閲覧可能な状態に置かれたものの、掲載を停止するまでの間に誰にも閲覧されていないことがアクセスログから明らかである場合などが考えられます。
69	個人情報保護委員会等への報告	意見⑧ （該当箇所） ２ページ・１７行目以降記載の、３．個人情報保護委員会等への報告 Ｐ３の、①実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合（※3） の記載事項に関し、 （意見） ・漏えい等事案に係る個人データ又は加工方法等情報によって特定の個人を識別することが漏えい等事案を生じた事業者以外ではできない場合（ただし、漏えい等事案に係る個人データ又は加工方法等情報のみで、本人に被害が生じるおそれのある情報が漏えい等した場合を除く。） に関し、 ここは、政府機関の情報セキュリティ対策のための統一技術基準（平成 24 年度版）　解説書（http://www.nisc.go.jp/active/general/pdf/K305-111C.pdf）等に、暗号とは異なるセキュリティ技術として秘密分散技術が具体的な利用シーンと共に記載公表され、要安定情報等の安全確保の手法として記載され公共等でも採用されてきたが、その対象となる技術標準化対象の秘密分散技術のうち、適切な当該技術等の利活用により法令の定義項から除外される特性を持つ秘密分散技術を、組織として適	本告示3.(2)①に規定する「漏えい等事案に係る個人データ又は加工方法等情報によって特定の個人を識別することが漏えい等事案を生じた事業者以外ではできない場合（ただし、漏えい等事案に係る個人データ又は加工方法等情報のみで、本人に被害が生じるおそれのある情報が漏えい等した場合を除く。）」とは、漏えい等事案が生じた個人情報取扱事業者において特定の個人を識別することができる情報であっても、第三者において特定の個人を識別することができない情報については、その漏えい等に係る個人情報保護委員会等への報告を要しないこととしたものです。ただし、仮に第三者において特定の個人を識別できない情報であっても、携帯電話番号のようにそれが利用された場合に本人が見ず知らずの者から不測の接触を受けるなど、その情報のみで本人に被害が生じるおそれのある情報の場合は除

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		切に安全管理措置を実施している場合に、該当させることができる条文と弊コンソーシアムでは認識しているが、いかがか？ また、括弧書き中の、～漏えい等事案に係る個人データ又は～、の記述は、例えばカード番号等で他の情報と照合することで本人特定に結びつく情報が想定されていると考えるが、記述が逆説的表現で理解しにくいので、少々修正してはいかがか。 （理由） 仮に秘密分散技術が高度な暗号化等の「等」の範疇に入る技術等の一つとして考えることができるのであれば、現場における現実的対策の一つとして利活用できると考えられるから。 【秘密分散法コンソーシアム】	くこととされています。 このように、御指摘の規定は、漏えい等事案に係る情報について暗号化等の秘匿化措置が講じられているか否かを問うものではありません。
70	個人情報保護委員会等への報告	意見⑨ （該当箇所） ２ページ・１７行目以降記載の、３．個人情報保護委員会等への報告 Ｐ３の、①実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合（※3） の記載事項に関し、 （意見） ・個人データ又は加工方法等情報の滅失又は毀損にとどまり、第三者が漏えい等事案に係る個人データ又は加工方法等情報を閲覧することが合理的に予測できない場合 に関し、 記述部分の意図としては、例えば細断や焼却による廃棄処理を想定しているものと考えるが、ここも秘密分散技術を適切に用いた際に、該当させることができるものと考える。秘密分散技術は、その技術処理の特性からして、対象電子データ等を意図的に廃棄状態にしていると言える処理であり、事実上対象電子データを滅失又は毀損させている処理と言える為、電子データの特性からして、適切な秘密分散技術を用いて処理し生成された割符ファイル単体から、個人データ又は加工方法等情報を閲覧することができない状態となる。解釈として問題あれば、ご指摘いただきたい。 （理由） 仮に秘密分散技術が高度な暗号化等の「等」の範疇に入る技術等の一つとして考えることができるのであれば、現場における現実的対策の一つとして利活用できると考えられるから。 【秘密分散法コンソーシアム】	本告示3.(2)①に規定する「個人データ又は加工方法等情報の滅失又は毀損にとどまり、第三者が漏えい等事案に係る個人データ又は加工方法等情報を閲覧することが合理的に予測できない場合」については、個人データ等が漏えいしていないと合理的に考えられる場合に限定されます。 実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
			鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。
71	個人情報保護委員会等への報告	意見⑩ （該当箇所） ２ページ・１７行目以降記載の、３．個人情報保護委員会等への報告 Ｐ３の、②FAX 若しくはメールの誤送信、又は荷物の誤配等のうち軽微なものの場合 （※4） の記載事項に関し、 （意見） （※4） なお、「軽微なもの」には、例えば、次のような場合が該当する。 ・FAX 若しくはメールの誤送信、又は荷物の誤配等のうち、宛名及び送信者名以外に個人データ又は加工方法等情報が含まれていない場合 に関し、 この部分も宛名書き以外の部分に関しては、適切な秘密分散技術によって宛名書き及び送信者名以外の個人データ又は加工情報等情報が割符化されており、復元に至らない数の割符ファイル又は、割符ファイル単体の中の無意味（法令の定義項から除外されるとこれまで貴委員会等に確認等してきた）なビットの羅列だけが含まれているのであれば要件を満たす記述と弊コンソーシアムでは考えるが、いかがか？ （理由） 仮に秘密分散技術が高度な暗号化等の「等」の範疇に入る技術等の一つとして考えることができるのであれば、現場における現実的対策の一つとして利活用できると考えられるから。 【秘密分散法コンソーシアム】	宛名及び送信者名以外に個人データ又は加工方法等情報を含むメールの誤送信等において、宛名及び送信者名以外の情報について高度な暗号化等の秘匿化がされていることによって、実質的に第三者が宛名及び送信者名以外の情報を閲覧することができない場合には、本告示 3.(2)②に規定する「FAX 若しくはメールの誤送信、又は荷物の誤配等のうち軽微なものの場合」に該当するものと考えられます。
72	個人情報保護委員会等への報告	○意見２ （該当箇所）２ページ　３－（１）報告の方法 （意見内容）「個人情報保護委員会の権限が事業所管大臣に委任されている分野における個人情報取扱事業者の報告先については別途公表するところによる」とあるが、クレジット会社のように、複数の事業領域にまたがるような場合（例：信用分野と金融分野）において、複数の報告先に報告を行うのではなく、主たる事業領域の報告先に報告すればよいようにしていただきたい。 （理由）例えば、クレジットカードに関する個人データの漏えいがあった場合においては、基本的に信用分野に従って報告を行うことになると考えられるが、一方で金融分野にも報告が必要である場	個人情報保護委員会の権限が事業所管大臣に委任されている分野における個人情報取扱事業者の報告先については、今後関係行政機関と調整のうえ、考え方を定める予定です。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		合は当該漏えいデータが金融分野に関する個人データとなるか否かを別途判断しなければならず、事業者にとって負担が大きい。 【日本クレジットカード協会】	
73	個人情報保護委員会等への報告	○意見５ （該当箇所）２ページ　３－（２）－１ （意見内容）「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合」の事例のうち、『個人データ又は加工方法等情報の滅失又は毀損にとどまり、第三者が漏えい等事案に係る個人データ又は加工方法等情報を閲覧することが合理的に予測できない場合』とは、例えば個人データを社内で誤ってシュレッダー廃棄した（もしくは廃棄した可能性が高い）場合を指すとの考え方でよいか。 【日本クレジットカード協会】	社内で誤って廃棄又は削除した場合には、「滅失又は毀損にとどまり、第三者が漏えい等事案に係る個人データ又は加工方法等情報を閲覧することが合理的に予測できない場合」に該当するものと考えられます。
74	個人情報保護委員会等への報告	○意見６ （該当箇所）２ページ　３－（２）－２ （意見内容）「ＦＡＸ若しくはメールの誤送信、又は荷物の誤配等のうち軽微なものの場合」に宛名及び送信者名以外の情報を「第三者に閲覧されないうちに（未開封で）全てを回収した場合」を追加していただきたい。 （理由）郵便等の誤配では、宛名等以外の個人データが含まれている場合が多く、報告を要しない要件、所謂、軽微なものに 「第三者に閲覧されないうちに回収した場合」を追記して頂かないと実務影響が大きいため。 【日本クレジットカード協会】	宛名及び送信者名以外の情報を第三者に閲覧されないうちに（未開封で）全てを回収した場合は、本告示3.(2)①に規定する「漏えい等事案に係る個人データ又は加工方法等情報を第三者に閲覧されないうちに全てを回収した場合」に該当するものと考えられます。
75	個人情報保護委員会等への報告	○意見７ （該当箇所）２ページ　３－（２）－２ （意見内容）「荷物の誤配」には、郵便の誤配が含まれるものと理解してよいか。 （補足）荷物の定義確認 【日本クレジットカード協会】	御理解のとおりです。
76	個人情報保護委員会等への報告	○意見３ （該当箇所）２ページ　３－（２）報告を要しない場合 （意見内容）漏えいをした情報が、公表情報（法人代表者名）等、漏えいだけで個人の権利利益を損ねる可能性が低い場合、報告対象外としていただきたい。 【日本クレジットカード協会】	公表情報の場合であっても、個別の事例ごとに判断して、漏えい等が発覚した場合に措置を講ずる必要がある場合もあり得るものと考えられます。いずれにしても御意見は今後の執務の参考とさせて頂きます。
77	個人情報保護委員会等への報告	○意見４ （該当箇所）２ページ　３－（２）報告を要しない場合 （意見内容）本人が事業者に連絡先の変更を申告する義務を怠ったことにより、誤配等が発生して事業者に責任がない場合も報告対象外としていただきたい。	御意見は今後の執務の参考とさせて頂きます。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		（理由）事業者に責のない場合は再発防止を行うことが実質不可能であり、これらを報告対象とすると事業者にとって負荷が大きいため。 【日本クレジットカード協会】	
78	個人情報保護委員会等への報告	（該当箇所） ２ページ、　「３．個人情報保護委員会等への報告」　のうち、「（１）報告の方法」部分 （意見） 要配慮個人情報についても通常の個人データと同じ報告方法でよいという理解でよいでしょうか。 （理由） 個人情報保護委員会が公表している「事業者における特定個人情報の漏えい事案が発生した場合の対応について」では、「特定個人情報に関する重大事案又はそのおそれのある事案が発覚した時点で、直ちにその旨を特定個人情報保護委員会に報告する」等とあり、「重大事案」の定義づけもされています。「個人情報」の取扱いにおける重大事案に関しても、直ちに個人情報保護委員会に報告して、当該重大事案について把握していただく必要があるのではないかと考えます。なお、現行の経済産業省ガイドラインでは、「機微にわたる個人データを漏えいした場合は経済産業大臣に逐次速やかに報告を行うことが望ましい」として、通常の個人データと、その扱いを別にしています。 【一般財団法人日本情報経済社会推進協会】	御理解のとおりです。認定個人情報保護団体から個人情報保護委員会等への報告の方法を含む運用の詳細については、認定個人情報保護団体とも調整の上対象事業者に示す予定です。
79	個人情報保護委員会等への報告	（該当箇所） ２ページ、　「３．個人情報保護委員会等への報告」のうち、 「（１）報告の方法」部分 （意見） 認定個人情報保護団体の対象事業者である個人情報取扱事業者が、当該認定個人情報保護団体に報告した場合、報告を受けた当該認定個人情報保護団体が行う行為についても、明記すべきではないでしょうか。あるいは、それらについては、完全施行前に、別途告示案等が示され、パブリックコメントが実施されると考えてよいでしょうか。 （理由） 同様の例として、特定個人情報に関する告示では、「２．本告示に基づく報告（１）報告の方法」の「ア」において、「（事業者からの事故報告を受けた）認定個人情報保護団体は、個人情報保護委員会に、その旨を通知する。」と記載されています。 【一般財団法人日本情報経済社会推進協会】	本告示の規定に基づき認定個人情報保護団体が対象事業者から漏えい等事案に係る報告を受けた場合、当該認定個人情報保護団体から当該報告について個人情報保護委員会等に報告していただくことになりますが、当該認定個人情報保護団体から個人情報保護委員会等への報告の方法を含む運用の詳細については、認定個人情報保護団体とも調整の上対象事業者に示す予定です。
80	個人情報保護委員会等への報告	（該当箇所） ２ページ、　「３．個人情報保護委員会等への報告」のうち、 「（１）報告の方法」部分 （意見） 事故報告書様式は、別途示されるのでしょうか。それは、いつごろどのような形で公開される予定	参考となる報告書の様式を、個人情報保護委員会のホームページに掲載する予定です。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		でしょうか。 （理由） 各省庁指定の様式を継承するのか、全体を統一化するのかによって、内部システムなどの改修等に時間を要し、新聞報道にあった5月30日完全施行に間に合わない可能性があります。 【一般財団法人日本情報経済社会推進協会】	
81	個人情報保護委員会等への報告	（該当箇所） ３ページ、　「３.(２) ①実質的に個人データ又は加工方法等情報が 外部へ漏えいしていないと判断される場合」 （意見） 「高度な暗号化等の秘匿化」とは具体的にどのようなものなのかについて、基準あるいは事例を示すべきではないでしょうか。 （理由） CRYPTREC暗号リスト（電子政府推奨暗号リスト）を指しているのであれば具体的に示しさないと事業者が理解できないと思います。特に、『個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）』のP4.21行目には「少なくとも、一般人及び一般的な事業者の能力、手法等を基準として当該情報を個人情報取扱事業者又は匿名加工情報取扱事業者が通常の方法により特定できないような状態にすることを求めるもの」としていますが、上記該当箇所の記述からすると、暗号化に関する専門的な技術知識を有しないと匿名加工情報が取り扱えない（高度な暗号化等の秘匿化ができないと漏えいリスクが高まる等）ようにも読めます。 【一般財団法人日本情報経済社会推進協会】	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。
82	個人情報保護委員会等への報告	（該当箇所） ３ページ、　「(2)報告を要しない場合」 （意見）	漏えい等事案に係る個人データ又は加工方法等情報を第三者に閲覧されないうちに全てを回収した場合、実質的に個人データ又は加工方法等情報が外部

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		「① 実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合」の事例として、個人データ又は加工方法等情報の滅失または毀損にとどまった場合は報告を要しないとされた理由は何でしょうか。 （理由） 個人データの滅失又は毀損にとどまった場合は、外部への漏えいとは異なり、当該個人に対して二次被害などの影響がないとのお考えから報告を要さない場合とされたのでしょうか。 個人データを滅失又は毀損することによっても、当該個人に対して、外部への漏えいと同等の深刻な不利益を与える場合もあると思われます。 【一般財団法人日本情報経済社会推進協会】	に漏えいしていないと判断され、また、実質的な被害がなく、その意味で漏えい等事案に係る影響度合いが限定的であると考えられることから、個人情報保護委員会等への報告を要しないものとしています。
83	個人情報保護委員会等への報告	（該当箇所） 3ページ (2) 報告を要しない場合　実質的に個人データ又は加工情報等情報が外部に漏えいしていない場合 （質問および要望） 質問1:「漏えい等事案に係る個人データ又は加工方法情報ついて高度な暗号化等の秘匿化がされている場合」には、生体認証で第一号個人識別符号を扱うことを想定すると、具体的にどのようなケースが当てはまるでしょうか。 以下に、該当すると想定する具体的な事例を挙げますので、ご回答をお願い致します。 さらにはガイドラインで具体的な要件を示していただくことにより、サービス提供者と利用者において適切な運用が可能となり、産業の振興にもつながると考えます。 想定事例１：生体情報保護技術（キャンセラブルバイオメトリクス、ファジィコミットメント、暗号化したままの登録用生体識別データと照合用生体識別データの照合等）が適切に用いられている場合。 想定事例２：生体情報保護技術を適用して、生体識別データを生成するときの条件（パラメータ）を変更して１つの生体情報から複数の異なる登録用生体識別データを生成できる仕組みを持ち運用している条件で、生成のための「条件（パラメータ）」は漏えいせずに登録データとしての生体識別データだけが漏えいした場合。（いわゆるキャンセラブルバイオメトリクスと言われる技術を用いていた場合。） 想定事例３：生体情報保護技術を適用して、生体識別データを生成するときの条件（パラメータ）を変更して１つの生体情報から複数の異なる登録用生体識別データを生成できる仕組みを持たせ、かつ、生体識別データ生成時に高度な不可逆処理を持たせて運用している条件で、生成のための「条件	生体認証保護技術であるテンプレート保護技術を施した個人識別符号について、高度な暗号化等の秘匿化がされており、かつ、当該個人識別符号が漏えいした場合に、漏えいの事実を直ちに認識し、テンプレート保護技術に用いる秘匿化のためのパラメータを直ちに変更するなど漏えいした個人識別符号を認証に用いることができないようにしている場合には、「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合」に該当し、個人情報保護委員会等への報告は不要と考えられます。 なお、本人への連絡等並びに事実関係及び再発防止策等の公表については、事案に応じて必要な措置を講ずることとされています。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		（パラメータ）」は漏えいせずに登録データとしての生体識別データだけが漏えいした場合。 想定事例４：生体情報保護技術を適用して、暗号化したまま登録データと照合データを照合できる生体認証システムにおいて、暗号化された登録用の生体識別データだけが漏えいした場合。 想定事例５：高度な不可逆処理を持たせた生体識別データに、生体識別データに由来しない秘密情報や個人情報を混ぜ合わせて単独では分離が困難な登録データとして保存し、本人の生体識別データを用いて照合した場合にのみ秘密情報や個人情報を取りだすことを可能にした生体認証システムにおいて、高度な不可逆処理を持たせた生体識別データに秘密情報や個人情報を混ぜ合わせて単独では分離が困難な登録データのみが漏えいした場合。 想定事例６：高度な不可逆処理を持たせた生体識別データに、生体識別データに由来しない秘密情報もしくは個人情報、および乱数を混ぜ合わせて単独では分離が困難な登録データとして保存し、本人の生体識別データを用いて照合した場合にのみ秘密情報や個人情報を取りだすことを可能にした生体認証システムにおいて、高度な不可逆処理を持たせた生体識別データに秘密情報や個人情報を混ぜ合わせて単独では分離が困難な登録データのみが漏えいした場合。 【一般社団法人日本自動認識システム協会】	
84	個人情報保護委員会等への報告	（該当箇所） 3ページ (2) 報告を要しない場合　実質的に個人データ又は加工情報等情報が外部に漏えいしていない場合 （質問および要望） 質問2:「個人データ又は加工方法等情報の滅失又は毀損にとどまり、第三者が漏えい等事案に係る個人データ又は加工方法等情報を閲覧することが合理的に予測できない場合」とは生体認証で第一号個人識別符号を扱う場合を想定すると、具体的にどのようなケースが当てはまるでしょうか。 以下に、該当すると想定する具体的な事例を挙げますので、ご回答をお願い致します。さらにはガイドラインで具体的な要件を示していただけると、適切な運用が可能となり、産業の振興にもつながると考えます。 想定事例１：生体情報保護技術を適用して、生体識別データを生成するときの条件（パラメータ）を変更して１つの生体情報から複数の異なる登録用生体識別データを生成できる仕組みを持ち運用している条件で、生成のための「条件（パラメータ）」は漏えいせずに登録データとしての生体識別データだけが漏えいした場合。	質問2については、いずれの場合も、個人識別符号に該当するものである場合には、個人データが漏えいしているため、「滅失又は毀損にとどまり、第三者が漏えい等事案に係る個人データ又は加工方法等情報を閲覧することが合理的に予測できない場合」には該当しないものと考えられます。 質問3については、実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となる

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		想定事例２：生体情報保護技術を適用して、暗号化したまま登録データと照合データを照合できる生体認証システムにおいて、暗号化された登録用の生体識別データだけが漏えいした場合。 想定事例３：生体認証に用いるデータの暗号鍵が利用システム毎に異なるものが用いられており、ある利用システムにおいて暗号鍵は漏えいせずに暗号化された登録生体情報のみが漏れた場合。 想定事例４：生体認証に用いるデータにおいて、システムに登録する登録用データと、利用者が認証の度に入力して生成する照合用データが異なっているシステムにおいて、登録用データのみが漏えいした場合。また、想定事例２と想定事例３の条件の組み合わせの場合。 想定事例５：生体識別データを端末に登録しての利用で端末を紛失した場合、その端末内の情報を登録する登録用データと、利用者が認証の度に入力して生成する照合用データが異なっているときに登録用データのみが漏えいした場合。 想定事例６：利用者のみの生体識別データを端末に登録しての利用で、利用者が端末を紛失した場合（端末の個人情報は端末利用時の識別用の生体情報のみ、登録データは暗号化）。 想定事例７：企業内の共用端末に置いて、利用者を含む従業員 10 名程度の複数人の生体識別データを端末に登録しての利用で端末を紛失した場合（端末の個人情報は端末利用時の識別用の生体情報のみ、登録データは暗号化）。 質問３：質問１と質問２では生体情報保護技術を前提とした質問を致しましたが、その他に高度な暗号化等としては、具体的にはどのような暗号化技術が高度と見なされるのでしょうか。また、「等」にはどのような手法が想定されますしょうか。 【一般社団法人日本自動認識システム協会】	ような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 　また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。 　また、生体認証保護技術であるテンプレート保護技術を施した個人識別符号について、高度な暗号化等の秘匿化がされており、かつ、当該個人識別符号が漏えいした場合に、漏えいの事実を直ちに認識し、テンプレート保護技術に用いる秘匿化のためのパラメータを直ちに変更するなど漏えいした個人識別符号を認証に用いることができないようにしている場合には、「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合」に該当し、個人情報保護委員会等への報告は不要と考えられます。 　なお、本人への連絡等並びに事実関係及び再発防止策等の公表については、事案に応じて必要な措置を講ずることとされています。
85	個人情報保護委員会等への報告	１．　本告示案３．（１）について 先般の個人情報保護法の改正の議論において個人情報保護委員会を設置する趣旨は、独立した第三者機関による分野横断的な統一見解の提示等を行うためとされている。 仮に、広範囲に渡る様々な分野において、個人情報保護委員会の権限の委任がなされるとすれば、改正前の個人情報保護法下の主務大臣制と同様の状況が生じ、個人情報保護委員会の独立性が事実上失われることとなり、個人情報保護委員会による分野横断的な個人情報保護という当初の目的が達成さ	権限の委任はあくまで事業所管大臣の専門的知見や体制を活用することが目的であり、現に当委員会から事業所管大臣に対して委任することができる権限は、報告徴収及び立入検査の権限に限られており、指導・助言・勧告・命令の権限は例外なく当委員会が実施するすることとされていることから、権限の

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		れないおそれがある。 本告示案において、権限が事業所管大臣に委任されている分野の個人情報取扱事業者の報告先については、「別途公表するところによる」とされており、権限の委任を前提とした記載となっているが、個人情報保護委員会の設置趣旨に鑑み、委任はあくまでも必要最小限度の範囲に止めるようにすべきである。 【アジアインターネット日本連盟】	一元化は適切に図られているものと認識しています。 なお、権限の委任は、改正後の法第 44 条第１項及び施行令第 12 条に基づき、①緊急かつ重点的に個人情報等の適正な取扱いを確保する必要がある場合、又は②効果的かつ効率的に個人情報等の適正な取扱いを確保するために事業所管大臣が有する専門的知見を特に活用する必要がある場合に限り行われることとされており、十分限定的に定められていると考えております。また、仮に事業所管大臣が報告徴収又は立入検査を実施した場合、その結果は当委員会に報告されることとされており、権限の一元化が適切に図られているものと考えられます。
86	個人情報保護委員会等への報告	２．　本告示案３．（２）②について 本告示案において、「報告を要しない場合」のうち、「FAX 若しくはメールの誤送信、又は荷物の誤配等のうち軽微なものの場合」の例として、「FAX 若しくはメールの誤送信、又は荷物の誤配等のうち、宛名及び送信社名以外に個人データ又は加工方法等情報が含まれていない場合」のみが例示されている。 あくまで例示である以上、上記の例示以外にも「軽微なもの」に該当する場合はあるという認識だがその点、明確にしていただきたい。また、報告を要しない「軽微なもの」は、「FAX 若しくはメールの誤送信、又は荷物の誤配等」の場合に限られる理由はないため、個別具体的な事情に照らして報告を要しない「軽微なもの」は本告示案３．（２）②記載の場合以外にもあるという認識だが、その点も明確にしていただきたい。 【アジアインターネット日本連盟】	いずれも御理解のとおりです。
87	個人情報保護委員会等への報告	本文において「個人情報取扱事業者は、漏えい等事案が発覚した場合は、その事実関係及び再発防止策等について、個人情報保護委員会等に対し、次のとおり速やかに報告するよう努める。」となっておりますが、その一方で「⑵ 報告を要しない場合　　次の①又は②のいずれかに該当する場合は、報告を要しない。」という記述があります。 そもそも努力義務として「努める」となっているものに対して「要しない」という用語が矛盾するように感じます。 義務規定「ねばならない。」に対する否定形として「要しない」であれば理解できますが、努力義務である「努める」であれば「要しない」ではなく「期待しない」「望まない」という用語になるかと考えます。	一般的に現状の案で御理解頂けるものと考えます。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		「⑵ 報告を要しない場合」は「(2)報告を望まない場合」「(2)報告をしてきて欲しくない場合」ということになりますか？ 【改正個人情報保護法　消費者志向で考える事業者ガイドライン研究会】	
88	個人情報保護委員会等への報告	「①実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合（※3）」の中で「・漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合」が示されています。 これまで経済産業省では、当該事案については「主務大臣等への報告」を促し、「本人への連絡」については省略して構わないとしてきました。 高度な暗号化等の秘匿化については、それが解読される可能性を経済産業省でもウォッチして事業者と連携を図って事故対応をして下さっていましたが、個人情報保護委員会では、暗号化等の信頼性については事業者が全ての責任を負うという考えで「(2)報告を要しない場合」とされたのでしょうか？ 【改正個人情報保護法　消費者志向で考える事業者ガイドライン研究会】	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。 このように実質的に個人データ等が外部に漏えいしていないと判断することが出来る程度の秘匿化がなされている場合には、軽微な事案として報告を要しないものとしています。
89	個人情報保護委員会等への	本文において「個人情報取扱事業者は、漏えい等事案が発覚した場合は、その事実関係及び再発防止策等について、個人情報保護委員会等に対し、次のとおり速やかに報告するよう努める。」となって	一般的に現状の案で御理解頂けるものと考えます。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
	報告	おりますが、その一方で「⑵ 報告を要しない場合　次の①又は②のいずれかに該当する場合は、報告を要しない。」という記述があります。 そもそも努力義務として「努める」となっているものに対して「要しない」という用語が矛盾するように感じます。 義務規定「ねばならない。」に対する否定形として「要しない」であれば理解できますが、努力義務である「努める」であれば「要しない」ではなく「期待しない」「望まない」という用語になるかと考えます。 「⑵ 報告を要しない場合」は「(2)報告を望まない場合」「(2)報告をしてきて欲しくない場合」ということになりますか？ 【公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会】	
90	個人情報保護委員会等への報告	「①実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合（※3）」の中で「・漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合」が示されています。 これまで経済産業省では、当該事案については「主務大臣等への報告」を促し、「本人への連絡」については省略して構わないとしてきました。 高度な暗号化等の秘匿化については、それが解読される可能性を経済産業省でもウォッチして事業者と連携を図って事故対応をして下さっていましたが、個人情報保護委員会では、暗号化等の信頼性については事業者が全ての責任を負うという考えで「(2)報告を要しない場合」とされたのでしょうか？ 【公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会】	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使でき

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
			ないように設計されていることのいずれかの要件を満たすことが必要と解されます。 　このように実質的に個人データ等が外部に漏えいしていないと判断することが出来る程度の秘匿化がなされている場合には、軽微な事案として報告を要しないものとしています。
91	個人情報保護委員会等への報告	（該当箇所） ３．個人情報保護委員会等への報告 （2）報告を要しない場合 ①実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合 ・漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合 （御意見） 次頁以降参照方 （理由） 次頁以降参照方 1. 情報漏えいの現実 　高度なデジタル社会の現代にあって、個人データを含む機密情報の情報漏えいが後を絶たない。その原因は情報技術の進化に伴い多様化しているが、とりわけモバイルパソコンの取り扱いによる情報漏えいが社会的にも大きなインパクトを及ぼしており、法人企業を中心に喫緊の対応が迫られている。 　第三者による不正アクセスや内部犯行が話題になりやすいが、モバイルパソコンを起因とする情報漏えいの現実として、所有者による当該端末の紛失・置忘れ（による情報漏えい）が最大の原因であることが挙げられる。 （図）（略） 2. 暗号化のリスク 　この現実に対し企業は手を拱いているわけではない。2016 年の調査（JIPDEC「企業 IT 利活用動向調査 2016」にみる IT 化の現状）によれば、企業の約半数以上がモバイルパソコンの社外持出しを禁止しており、またパソコンのハードディスクにデータを格納しない「シンクライアントシステム」の導入も約３割に至っている。しかしながらいずれの対策もモバイルパソコンがもたらす、いつでもどこでも効率的に仕事ができるという本来の生産性を阻害するものであり、現内閣が推進する「働き方改革」を抑制する一因とは言えまいか。	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 　第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストや ISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 　また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		これに対し約半数近い（同調査）企業が導入しているハードディスクないしはファイルの暗号化ツールであるが、米国標準暗号である AES（Advanced Encryption Standard）に代表される暗号化方式も既に Biclique 攻撃といった解読するための総当たり攻撃に必要な計算量を低減できるアルゴリズム上の脆弱性 などが指摘されており、何よりも情報の原本性がそこ（ハードディスク上）に留まる以上、暗号化による情報漏えいのリスクは完全には払拭できないと考える。 これは「暗号危殆化」として IPA（独立行政法人情報処理推進機構）などが既に指摘し、報告している通りであり＊1、XXXXXXXXXXXXXXXXXXXXXXXXXXX の報告では、暗号危殆化のリスクとして「暗号化、認証における安全性が失われ、情報漏洩の危険が生じる。例をいくつか挙げる。共通鍵暗号が危殆化すると、暗号化された情報を第三者に解読される『盗聴』の危険性が高まる。公開鍵暗号やデジタル署名が危殆化すると、本来のサーバのふりをする『なりすまし』を検証できなくなる危険性が高まる。ハッシュ関数が危殆化すると、通信の内容を書き換える「改ざん」の危険性が高まる。このような脅威が暗号アルゴリズムの危殆化によって発生する可能性がある」と指摘されている＊2。 ＊1（「暗号の危殆化に関する調査報告書」https://goo.gl/QHVhwg） ＊2（「暗号危殆化に対する HTTPS 暗号可視化手法の提案」より引用 https://www.jstage.jst.go.jp/article/jasi/26/0/26_0_335/_pdf） また一部の中央官庁においては特に個人情報の取り扱いについて暗号化が必ずしもこれを秘匿化するに十分なものではない旨を示唆する見解を示している。 ● 経済産業省「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212guideline.pdf） P2 の 2-1-1.「個人情報」の付帯説明内（下線は筆者による） 「『個人に関する情報』は、氏名、性別、生年月日等個人を識別する情報に 限られず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化等によって秘匿化されているかどうかを問わない」 ● 金融庁「金融機関における個人情報保護に関する Q&A」（http://www.fsa.go.jp/news/19/20071001-3/01.pdf） P13 の④（下線は筆者による） 「個人データ」の「漏えい」とは「個人データが外部に流出すること」であり、たとえ流出した媒体において暗号化処理がされていたとしても、「個人データ」の「漏えい」に当たります。また、暗号化処理ではなく、パスワードが設定されている場合も同様です。 さらには、暗号化に伴う鍵情報としてこれまで汎用的に用いられてきた「パスワード」も、その管理工数のわりに盗難や不正複製されるといったリスクが高い。世界が FIDO に代表される多要素認証	

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		をパスワードに代わる新しい認証技術と して、その標準化を急速に進めているのはその証左であろう。まさに XXXXXXXXXXXX が指摘したように、「パスワードはもはや迫り来る（セキュリティ）脅威に対応できない」*3 のである。 ＊3（“UK to invest $2.3B in cybersecurity, calls for stronger authentication”より 引用“passwords are no longer adequate as threats against them increase.” https://goo.gl/2l5QqJ） 3. 秘密分散によるセキュリティ 　翻って昨今、機密情報を秘匿化する新しいアプローチとして秘密分散技術が注目されている。この技術そのものは 1970 年代から主に米国にて研究されてきたが、コンピュータの進化に伴い電子割符としての実用化が進み、市場に おいてもこの技術を応用したアプリケーションやサービスが展開され始めてきた。 　こうした流れを受け、政府系機関ならびにその外郭団体においても秘密分散 技術を認め、推奨する動きが見られている。 ● 内閣サイバーセキュリティセンター（NISC）「政府機関の情報セキュリティ対策のための統一管理基準解説書」（http://www.nisc.go.jp/active/general/pdf/K304-101C.pdf） P61 の 1.3.1.4 (5)(f)（下線は筆者による） 行政事務従事者は、要機密情報である電磁的記録を移送する場合には、必要な強度の暗号化に加えて、複数の情報に分割してそれぞれ異なる移送経路を用いること 。 解説 : 情報を分割し、これを異なる経路で移送することを求める事項である。要機密情報を移送する場合には、当該要機密情報が情報量的に解読不能となるように、分割して移送を行うこと。この考え方は、専門用語で秘密分散技術といわれ 、例えば、1 個の電子情報についてファイルを 2 個に分割し、それぞれ暗号化を施した上で一方を電子メール、他方を CD-R、DVD、MO、USB メモリ、フラッシュメモリ等の外部電磁的記録媒体で郵送する方法が挙げられる。 ● 日本情報経済社会推進協会（JIPDEC）「電子記録管理に関する調査検討報告書 2014」（https://www.jipdec.or.jp/archives/publications/J0005038） P27 の 3.3 個人情報の非個人情報化（下線は筆者による） 秘密分散技術により 、個人情報や特定個人情報を処理し生成された個々の割符ファイルを適切に管理することにより、個々の割符ファイル単体は個人情報保護法、マイナンバー法（番号法）の対象外（非個人情報化）にすることができる ため、単体からの復元可能な情報も含む完全な情報を一元管理するような通常の情報管理に比べ、情報漏えい等に対する耐性を向上させ、事故発生によるリスク顕在化を未然防止する だけでなく、対象情報の委託・受託時の監督責任や管理責任を全うする際にも役立つ。また副次的効果として、割符ファイル単体が法令上の定義項から除外される ことから、海	

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		外のサーバに単体の割符ファイルを置くことも可能になる。 秘密分散方式の中でもとりわけ AONT（All Or Nothing Transform）と呼ばれる方式は文字通り分散した割符がすべて（All）揃わなければ、決して復元が成立しない（Nothing）ものであり、暗号化が留める（機密情報の）原本性を秘密分散により喪失たらしめるものであるから、そのセキュリティ強度は比類なきほどに高い（当社比、6 ページ「別紙」参照方）。またすべての割符が揃うことそのものが復元の絶対要件であることから、暗号を復号するための鍵ならびにパスワードという要件が秘密分散（AONT）には存在せず、したがい前述のこれに係るリスクも存在しない。 例えば当社が提供する“XXXXXX”は、AONT 方式を採用した極めて高度なセキュリティ技術と高いユーザビリティを両立したアプリケーションであり、特にモバイルパソコンの機密情報セキュリティを対象とした“XXXXXXXXXXX”はユーザーの生産性を犠牲にすることなく、個人データをはじめとする機密情報を AONT 方式の秘密分散技術により原本性残存のリスクを払拭し、極めて堅牢なセキュリティでこれを秘匿化することを実現しており、日本を代表するグローバル IT 企業である XXXXXXX も暗号化に代わるソリューションとしてこれを全社的に採用した。 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX 4. 意見 このたびの「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（案）」においては、漏えい等事案が発覚した場合、実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合の一例として「漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合」は個人情報保護委員会に対する報告を要しない旨の案が提起されているが（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（案）3.(2)①)、いわゆる AES に代表される暗号化が「高度な暗号化」に該当する場合、前述の情報漏えいリスクを孕んでいるのであるから（実質的に外部に漏えいするリスクを払拭できていないのであるから）、報告を要しないとする判断は軽軽に行われるべきものではない。 翻って、今後の改正個人情報保護法施行を見据え、ビックデータ活用の推進や小規模取扱事業者への対応を鑑みるならば、堅牢性と可用性を兼ね備えた秘密分散技術によってはじめてこのリスクが払拭されるため、当該条件文の「高度な暗号化等の秘匿化がされている場合」は「秘密分散等の技術を組み合わせた高度な暗号化の秘匿化がされている場合」（下線は筆者による）と当該リスクの回避方法を具体的に明示した上で報告を要しないとされるべきである。 以上 （別紙）（略） 【株式会社 TCSI】	

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
92	個人情報保護委員会等への報告	「３．個人情報保護委員会等への報告　（２）報告を要しない場合」の一例として、「漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合」と示されているが、例えばハッシュ化して各種データを保存している状況において、ソルトやストレッチングなどの手法を用いてハッシュ化していなかった場合、さほどのコスト、リソースを用いなくても漏えいデータは容易に復元されてしまうと思われる。 よって、「漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がなされている場合」の文言については、この文言によって事業者より報告がなされないことを避けるためにも、削除することが望ましいと考える。 【一般社団法人 JPCERT コーディネーションセンター】	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。
93	個人情報保護委員会等への報告	該当箇所 3-(2)① 漏えい等事案に係る個人データ又は加工方法等情報によって特定の個人を識別することが漏えい等事案を生じた事業者以外ではできない場合（ただし、漏えい等事案に係る個人データ又は加工方法等情報のみで、本人に被害が生じるおそれのある情報が漏えい等した場合を除く。） 意見 但し書きで指している情報が不明瞭のため、具体的な例を示していただきたい。 提出理由	漏えい等事案に係る個人データ又は加工方法等情報の内容や性質等を勘案して個別の事例ごとに判断することとなりますが、例えば、携帯電話番号のようにそれが利用された場合に本人が見ず知らずの者から不測の接触を受けるなど、その情報のみで本人に被害が生じるおそれのある情報が該当すると考えられます。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		報告要否の観点から確認したい。 【SMBC コンシューマーファイナンス株式会社】	
94	個人情報保護委員会等への報告	（該当箇所） 3 ページ・ 24 行目以下 3.個人情報保護委員会等への報告 (2)報告を要しない場合 ②FAX 若しくは メールの誤送信、又は荷物の誤配等のうち軽微なものの場合（※4）について （意見） 1)「(2)報告を要しない場合②」の見出しから「FAX 若しくはメールの誤送信、又は荷物の誤配等のうち」を削除することを提案し、 2)②に該当するケースは※4 記載の例に限定されず、(1)対象の個人情報が名前のみではないケース、(2)個人情報の本人が 1 名のみではないケースであっても②に該当する場合もあることをご確認いただくよう要望します。 （理由） 「(2)報告を要しない場合②」の見出しに「FAX 若しくはメールの誤送信、又は荷物の誤配等のうち」と記載されているところ、※4 記載の例に同じ記載があり記載が重複する上、個人データの漏えいが軽微な場合は他にあるため、上記意見 1)のとおり提案いたします。 また、原案の書き振りでは②に該当し報告を要しない場合が具体的に例示されているため、例示ではあるものの、個人情報の範囲および本人の数が記載の例より少しでも拡がれば、これに該当しないと解釈できることを懸念しています。例えば、企業から消費者宛に荷物を発送する際、伝票が誤って他の消費者宛の伝票と重ねて貼り付けられ配送されたケース（宛名および送信者名以外に住所も含まれる場合）、さらに、複数の伝票が誤って添付され配送されたケースであっても報告を要することとなるようにも読めるため。 【在日米国商工会議所】	本告示 3.(2)②の見出しから「FAX 若しくはメールの誤送信、又は荷物の誤配等のうち」を削除した場合、個人情報保護委員会等への報告を要しない場合が過度に拡大することとなり、適切でないと考えます。 なお、本告示 3.(2)②※4 に例示するもののほか、個人情報保護委員会等への報告を要しないものと考えられる事例について、Q&A において考え方を示してまいります。
95	個人情報保護委員会等への報告	■該当箇所 3 ページ・「(2)報告を要しない場合」 ■意見（賛同） 官庁等への報告を要しない軽微基準の明確化については、2005 年 4 月の現行法全面施行以来、JEITA としても再三にわたり要望してきたところであり、このたび、委員会告示として明確化されたことは、強く賛同する。	賛同の御意見として承ります。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		今後とも、認定個人情報保護団体を含めて過剰な報告義務を事業者に対して課す事がないようご指導いただくことを要望する。 ■理由 従来の省庁ガイドラインでは、主務大臣に報告を要しない軽微基準が明確でなかったり、場面が極めて限定されていたりして、事業者側にとって過重な負担となっていた。 今回、明示された軽微基準は、本人の権利履歴の侵害につながるリスクがほとんどない事例に限られており、極めて妥当な基準であると考えられるため。 【一般社団法人　電子情報技術産業協会】	
96	個人情報保護委員会等への報告	「漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合」とはどの程度のレベルを言うのか。 ※例として市販の暗号化ソフトで暗号化のうえ、データの復号に英数混合１０桁のパスワードが設定されている場合は「秘匿化」がされていると考えてよいのか。 【個人】	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。
97	個人情報保護	高度な暗号化。。。は何をもって高度な暗号というのでしょうか。データの保管時における暗号化アル	実質的に個人データ又は加工方法等情報が外部に

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
	委員会等への報告	ゴリズム vs データ転送時における暗号化アルゴリズム、鍵長などを明記頂けると、良いかと思われます。 また、貴委員会への連絡が必要な情報流出の場合、監督庁への連絡についても同様になりますか？その場合、監督庁への連絡をする・しない判断についても本ガイドラインを参考にしてもよいのでしょうか？ 【個人】	漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。 このような場合には、実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断されることから、個人情報保護委員会等への報告を要しないものとしています。
98	個人情報保護委員会等への報告	（該当箇所）3 ページ (※3) 3 行目「漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合」 （意見）漏えい等事案が発覚した時点では「秘匿化がされている」ため報告を要しなかったものが、後に新たな技術の出現・普及等により秘匿を容易に破ることが可能となった場合、改めて報告の対象になるのかを確認したい。	漏えい等事案が生じた当時の技術水準に照らして、実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合には、個人情報保護委員会等への報告を要しないものと考えられます。なお、「高度な暗号化等の秘匿化がなされている場合」の考え方に関する Q&A の内容は技術の進

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		（理由）量子コンピュータの実用化や、暗号方式が依拠する予想の否定的解決、暗号化アルゴリズムの脆弱性発見などにより、短期間で秘匿化が「高度」でなくなる事態は考えられるため。 【個人】	展等を踏まえ見直される場合がありますので、最新の Q&A を御参照下さい。
99	個人情報保護委員会等への報告	以下、案について意見を行う。 この様な報告の定めを行うのは望ましいと考える。 しかし、例えば、検察や警察における、加害者側への被害者情報の漏洩は結構すさまじいのであるから（組織犯罪者に甘い態度に加え、被害者側の情報漏洩を常習としているのは、市民にとって悪夢的である。逆に本人情報の開示は不合理な程度に拒絶的なのであるが。不合理な不正義な組織である。）、本気で対策を打つためには、検察や警察を叩く覚悟が必要であると当方は考える。 内容については概ねよいのではないかと思われたが、以下、注意したい事があるので意見を行う。 3.(2).〇1.の(※3)について ・「高度な暗号化」については「高度な暗号」が既に信用出来ない世の中となっているので、記述は止めた方がいいと考える（高強度とされる暗号でも、数万台規模のクラスタ計算機や、既に一昨年あたりから google 社が実用に供している量子計算機（例えば D-Wave 社のもの）をもって解析を行ったのであれば、「実用的」な時間で解析が行われてしまう可能性が高いと認識すべきであると考える。）。この様な記述が行われていた場合、それを口実に「暗号化」（ただし解かれてしまうと分かっているもの）したデータが故意に流出させられても、それを個人情報保護委員会や上級庁が知る事が無くなってしまうのであるが、それは非常に問題であるはずである。であるので、「高度な暗号化等の秘匿化がされている場合」の記述については削除されたい。 ・「第三者に閲覧されないうちに全てを回収した場合」という項目については、当然その保証が行えないので、これはインシデントとして報告させるようにしていただきたい。 ・「特定の個人を識別することが漏えい等事案を生じた事業者以外ではできない場合」というものについてもインシデント報告させるべきであると考える。これを許容してはならないはずである。 この部分（「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合」）について、一概に言って、案ではあまりにも犯罪者に逃げ口を与えすぎていると思われるのであるが、相手は概ね広域な組織犯罪者（しかも資金力も兆円規模といったものであろう。厚生労働省所管分野事業からの無駄な支出は１年で兆を越えるし、各種経済活動における組織的不正は数多い（東京五輪だってどのくらい多くの不正が発見されているであろうか。）。非常に強大な資金力（及びそれにものを言わせた技術力）とコネを駆使してくる相手と対峙しなければならない事を認識すべきであると考える。）であるので、漏れた情報はほぼ全てが照合され利用されると認識すべきであると考える。よって、「漏えいしていないと判断される場合」はもっと範囲を狭めていただきたい。（でなければ、組織内の内通者が「仕事」をし放題になってしまうと考える。）	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストや ISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		意見は以上である。 【個人】	
100	個人情報保護委員会等への報告	２．漏えい等事案が発覚　した場合に講ずべき措置 （1）報告の方法 質問１ 「個人情報保護委員会の権限が事業所管大臣に委任されている分野の詳細 」に関しては「別途公表するところによる」とある。 既に発表されているなら具体的な文書名やリンクをお教え願いたい。 また、未発表であるならば公表時期をお教え願いたい。 質問２ 特に認定個人情報保護団体の対象事業者になっていない場合は 貴委員会に報告するという理解でよいか。 またその場合の報告フォーム等は規定が何か既に存在するのか 【匿名】	質問１については、委任先となる関係行政機関との調整が完了し次第、個人情報保護委員会のホームページへの掲載等の方法により速やかに公表する予定です。 質問２については、御理解のとおりです。参考となる報告書の様式を、個人情報保護委員会のホームページに掲載する予定です。
101	個人情報保護委員会等への報告	いつもお世話になっております。 念のため確認でございますが、各分野の統一的な報告様式を作る予定はあるのでしょうか。報告の様式は任意となるのでしょうか。 【匿名】	参考となる報告書の様式を、個人情報保護委員会のホームページに掲載する予定です。
102	個人情報保護委員会等への報告	主文 ３頁　※３中の第１項目を抹消する。 理由 「・（前略）高度な暗号化等の（後略）」とあるが、『高度』の定義が無い。漏洩企業が批判を恐れるあまり安易に、かつ自己判断で「高度」とする可能性が否定できず、被害者保護の観点から逆行する。 「自己判断」が多大な問題を含有することはＷＥＬＱ騒動で証明済みである。 補足資料 最近一部ブラウザでは非推奨とされたＳＳＬ方式においても、少々のＩＴスキルでは解読できるものではなく、現状でも一定高度の暗号化システムである。そのうえでなお、「より安全な」方式への移行を推奨する意味で非推奨とされているにすぎない。 【匿名】	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されているこ

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
			とが考えられます。 　また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。 　このような場合には、実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断されることから、個人情報保護委員会等への報告を要しないものとしています。
103	個人情報保護委員会等への報告	スマートフォンではパスワードを使用しない「安全な」認証技術として FIDO があるが、これは端末内に生体情報を秘匿化して格納している。 認証の仕組みとしては安全な手法だと言えるが、端末を紛失すると個人情報漏洩となってしまうのか？ FIDO 等のローカル認証用の生体情報は、端末内ではごく少数の利用者の情報に限られそれ自体を流用される可能性も低いため漏洩事故の対象にすべきでないと考えます。 【匿名】	生体認証保護技術であるテンプレート保護技術を施した個人識別符号について、高度な暗号化等の秘匿化がされており、かつ、当該個人識別符号が漏えいした場合に、漏えいの事実を直ちに認識し、テンプレート保護技術に用いる秘匿化のためのパラメータを直ちに変更するなど漏えいした個人識別符号を認証に用いることができないようにしている場合には、「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合」に該当し、個人情報保護委員会等への報告は不要と考えられます。 　なお、本人への連絡等並びに事実関係及び再発防止策等の公表については、事案に応じて必要な措置を講ずることとされています。
104	個人情報保護委員会等への報告	報告対象外となる要件が非常に不明瞭な点を懸念しています。 情報漏洩で特に多いのが、ファイルが流出する事案です。 この時、たとえ AES256 の暗号化がなされていても、その手法が ZIP 化＋パスワードであれば、これは高度な暗号化とは程遠いです。通常、ファイルとともにパスワードも流出するからです。 報告対象として、このように多く発生するであろう「暗号化自体は高度だが、手法がパスワード管理」というものは、漏洩対策としては不十分であり、高度な暗号化という要件を満たさない点を明記する	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難とな

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		必要があると考えます。 AES256 自体は政府推奨暗号にも採用されているため、AES256 だからファイルが漏洩しても報告しない、という事案が増えることを懸念しています。 【匿名】	るような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。
105	個人情報保護委員会等への報告	報告対象外となる要件が非常に不明瞭な点を懸念しています。 情報漏洩で特に多いのが、ファイルが流出する事案です。 この時、たとえ AES256 の暗号化がなされていても、その手法が ZIP 化＋パスワードであれば、これは高度な暗号化とは程遠いです。通常、ファイルとともにパスワードも流出するからです。 報告対象として、このように多く発生するであろう「暗号化自体は高度だが、手法がパスワード管理」というものは、漏洩対策としては不十分であり、高度な暗号化という要件を満たさない点を明記する必要があると考えます。 AES256 自体は政府推奨暗号にも採用されているため、AES256 だからファイルが漏洩しても報告しない、という事案が増えることを懸念しています。 【匿名】	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されているこ

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
			とが考えられます。 　また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。
106	個人情報保護委員会等への報告	高度な暗号化等の秘匿化がされている場合は委員会への報告が不要となっているが、本人に対する通知または公表を不要としているわけではない旨の注記が必要。 また、「高度な暗号化等」の具体例が必要。 【匿名】	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 　第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 　また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
			満たすことが必要と解されます。
107	個人情報保護委員会等への報告	３．個人情報保護委員会等への報告 （２）報告を要しない場合 「実質的に個人データ又は加工等情報が外部に漏えいしてないと判断される場合」 質問１ 「高度な暗号化」とは具体的にどのレベルまでの実装をすれば満たされるのか？ 「電子政府における調達のために参照すべき暗号のリスト 」等は存在するが あくまで政府機関の情報セキュリティ対策を目的としており民間の実情とは そぐわない可能性がある。 暗号化形式の明確な推奨を希望する。 質問２ 滅失または毀損のみである場合は報告の要はない旨の記載がある。 漏洩時のみ報告するという理解でよいか。文書中にて明記してほしい。 （DB テーブルの一部破損等も 滅失または毀損 の対象とされた場合、負荷が高いため） 質問３ 「 １．対象とする事案 」においては （１）においては「個人データ」に関しては漏えい、滅失又は毀損を対象としているが、 （２）において「個人情報取扱事業者が保有する 匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号 」と「 加工方法等情報 」は 漏えいのみを本告示の対象としている。 報告すべき対象は 「個人データ」、 「個人情報取扱事業者が保有する 匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号 」ともに漏えい時のみであるなら 「 １．対象とする事案 」の（１）において漏えいのみならず、滅失又は毀損を記載している理由が不明である。 理由があればご教示願いたい。また必然性が無い場合は両箇所の記述を揃えてほしい。 FAX 若しくはメールの誤送信、又荷物誤配等のうち軽微なものの場合 質問 誤配の結果、本来の宛先人以外が開封し、荷物の内容を認知した場合は 軽微にあたるか。 荷物の内容は千差万別であり、一概の判断は困難かと思うが 内容物そのものが購買の履歴となるケースもある。 また単なる販促内容の文書のみであれば実質的に宛名以外に漏えいはないものと思われる。	質問１については、実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。 質問２については、御理解のとおりです。一般的に現状の案で御理解頂けるものと考えます。 質問３については、個人データの滅失又は毀損のみにとどまり、第三者が漏えい等事案に係る個人データ又は加工方法等情報を閲覧することが合理的に予測できない場合、個人情報保護委員会等への報告は要しないものとしても、本告示２．に規定する漏

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		考え方の基準を示してほしい。 【匿名】	えい等事案が発覚した場合に講ずべき措置が個人情報取扱事業者において講じられることは望ましいと考えられるため、本告示１．(1)において、「滅失又は毀損」と規定することとしています。 FAX 若しくはメールの誤送信、又は荷物誤配等のうち軽微なものの場合の質問については、一般に、本来の宛先人以外の者によって開封され、荷物の内容が認知された場合であっても、当該内容に個人データ又は加工方法等情報が含まれない場合には、本告示に基づく個人情報保護委員会等への報告を要しないものと考えられます。
108	個人情報保護委員会等への報告	※３の箇条書き２個目について、たまたま第三者に閲覧されないうちに全て回収したとしても、漏えいをしたことは管理状況が悪いことを示す重要な事柄なので、報告することにするべきである。 【匿名】	漏えい等事案に係る個人データ又は加工方法等情報を第三者に閲覧されないうちに全てを回収した場合、実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断され、また、実質的な被害がなく、その意味で漏えい等事案に係る影響度合いが限定的であると考えられることから、個人情報保護委員会等への報告を要しないものとしています。
109	個人情報保護委員会等への報告	（該当箇所） 3 ページ 5 行 （意見） 個人情報取扱事業者は漏えい等事案が発覚した場合は、その事実関係及び再発防止策等について、個人情報保護委員会等に対し、次のとおり速やかに報告するよう努める。として、3.(2)に報告を要しない場合として事例が提示されています。 3.(2)1，2 についても報告は受けるようにご検討いただけないでしょうか。ただし、再発防止策まで報告を求めると個人情報取扱事業者の負担になるため、その事実関係だけの報告とし、報告の方法や報告内容を軽減し次のような手続きにできないでしょうか？ ・3.(2)1 については、「事実関係」及び「再発防止策等の報告を免れる理由」を記載し報告する。 ・3.(2)2 については、「事実関係」及び「再発防止策等の報告を免れる理由」を記載し、月ごとにまとめて報告することができる。 （理由） 私共、業界団体は個人情報取扱事業者から事故情報を受け付け、主務大臣に報告しています。業界団体として漏えい等事案が発覚した場合には、全ての事案を収集しヒヤリ・ハット対策として公表し、	本告示に規定する個人情報保護委員会等への報告を要しない場合に該当する漏えい等事案であっても、個人情報取扱事業者が必要と判断する場合には、本告示の規定にかかわらず、個人情報保護委員会等へ報告することができます。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		業界での再発防止に努めております。従来は3.(2)1，2についても報告を求め、同業種間等で当該事案に関する情報を共有して、再発防止を図っています。 【匿名】	
110	個人情報保護委員会等への報告	※4について、誤送信によって、これこれの宛先にこれこれの内容が連絡されているのだと他者に知られることは、本来の宛先の者にとって重大な問題なので、「軽微」としているのは、おかしい。 【匿名】	従前の主務大臣が制定するガイドラインにおける取扱いを参考にして、FAX 若しくはメールの誤送信、又は荷物の誤配等のうち、宛名及び送信者名以外に個人データ又は加工方法等情報が含まれていない場合のように軽微な事案については報告を要しないものと規定しています。
111	個人情報保護委員会等への報告	※4に出てくる「宛名」が、氏名・名称だけ、または、FAX 番号だけ、E メールアドレスだけを指しているのか、「FAX 番号・氏名」「E メールアドレス・氏名」「住所・氏名」といった各セットも指しているのかなど、何を指しているのかわからないので、わかるように記述するべきだ。 【匿名】	一般的に現状の案で御理解頂けるものと考えます。
112	その他	・本告示のパブリックコメントは行政手続法に基づくものとされているが，行政手続法の「命令等」（行政手続法２条８号）のうち①法律に基づく命令，②審査基準，③処分基準，④行政指導指針のいずれの法的性質を有するものか，回答されたい。 【金融機関における個人情報の実務研究会】	御意見は、本意見募集の対象外と考えますが、行政指導指針に該当するものと考えられます。なお、安全管理措置に違反していると認められる場合には個人情報保護法に基づき適切な監督が行われることとなります。
113	その他	・特定個人情報告示は改正法施行にあわせて改正する予定はないか，回答されたい。特に，特定個人情報告示２（２）では，「個人情報取扱事業者以外の事業者」が名宛人とされているが，改正法施行により中小規模事業者も個人情報取扱事業者とされる以上，それに対応した改正は不可欠なように思われるところ，改正しないのであれば改正しない合理的理由について説明されたい。 【金融機関における個人情報の実務研究会】	御意見は、本意見募集の対象外と考えますが、「事業者における特定個人情報の漏えい事案等が発生した場合の対応について（平成 27 年特定個人情報保護委員会告示第２号）」については、今後、改正する予定としております。
114	その他	・本告示１（１）につき，あるデータが「個人データ」かどうかはどのように判断されるのか回答されたい。例えば，特定の個人を識別することができるのが漏えい元の個人情報取扱事業者のみで，漏えい先の第三者には特定の個人を識別することができない場合には，本告示１（１）の「個人データ」ではないということでよいか，回答されたい。 【金融機関における個人情報の実務研究会】	御意見は、本意見募集の対象外と考えますが、ある情報が「個人データ」に該当するか否かについては、法第２条の規定に従って判断されます。
115	その他	（該当箇所） パブリックコメントが行われている告示案全体 （意見） 当該告示案は、個人情報保護委員会より、個人情報取扱事業者に向けた「漏えい等の事案が発生した場合等の対応について」記載されています。一方で、改正個人情報保護法では、この漏えい等の事案発生の報告を受けた場合を含め、認定個人情報保護団体を通じた対応もあると考えられます。完全	本告示の規定に基づき認定個人情報保護団体が対象事業者から漏えい等事案に係る報告を受けた場合、当該認定個人情報保護団体から当該報告について個人情報保護委員会等に報告していただくことになりますが、当該認定個人情報保護団体から個人情報保護委員会等への報告の方法を含む運用の詳細に

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		施行までに認定個人情報保護団体に向けた同様の告示（案）等が個人情報保護委員会から示され、パブリックコメントが行われると考えてよいでしょうか。 （理由） 改正保護法において、認定個人情報保護団体に求められる責務もあると考えられるため。 【一般財団法人日本情報経済社会推進協会】	ついては、認定個人情報保護団体とも調整の上対象事業者に示す予定です。
116	その他	意見⑪ （該当箇所） １ページ・１行目以降記載事項全般に関し、 （意見） 昨今のサイバー攻撃は、狙われれば必ず侵入されると考えざるを得ないレベルとなっており、侵入されたとしても被害（実害）を最小化できる対策が急務。またＡＩの進化と共に機械的学習によりビッグデータも攻撃者の有効な情報源となることを踏まえると、本当に報告しなくても良い。と、現場判断できる基準の整備が肝要と考えるが、いかがか。その意味では、当パブコメに対応して具体的且つ現実的に参考となる技術や対策、事例等が公表され、そうした対策等を適切に実施している場合には、当パブコメのように「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合」に該当するものとして、「⑵ 報告を要しない場合」との判断を現場で行うことは、現場実務上大いに意義があるものと考える。 そこで、事故発生時に法令解釈上も本当に役立つ技術的対策や参考事例等の資料等が貴委員会より公開されると広く社会に役立つと考えるが、いかがか？ （理由） 昨今の事件等は攻撃手法が高度化としていると同時に、組織化と一般化、グローバル化、更に低年齢化も急激進んでいる。ＥＵ等とのデータ交換等に必要なプライバシー保護の観点からも、国際社会でも評価される現場における現実的法令対処に向けた対策等の指針が、日本発で示されることが、国内事業者等の法令対処のみならず、日本の発展的未来に貢献すると考えるから。 【秘密分散法コンソーシアム】	実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。 また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。
117	その他	個人情報取扱事業者 には、地方公共団体は含まれないようだが、個人情報の取扱いについては、地方公共団体についても対象にすべきではないか。 マイナンバーを含む個人情報は、別の規定により、報告対象のようであるが、マイナンバーがあろうなかろうと個人情報は大事な情報であり、個人情報保護委員会で、一括して管理すべきではないか。	御意見は、本意見募集の対象外と考えますが、御指摘の内容については、今後の執務の参考とさせて頂きます。

No	該当箇所	寄せられた御意見等	御意見等に対する考え方
		【匿名】	

（注）寄せられた御意見等につきましては、特定の個人や店舗等の識別につながるおそれのある箇所を一部編集して掲載しているものがあります。