「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」改正案の新旧対照表

（傍線部分は改正部分）

○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

改　正　案	現　行
2-2-2.個人情報の取得関係（法第１７条～第１８条関連） （１）適正取得（法第１７条関連） 法第１７条 （略） 個人情報取扱事業者は、偽り等の不正の手段により個人情報を取得してはならない。 なお、不正の競争の目的で、秘密として管理されている事業上有用な個人情報で公然と知られていないものを、不正に取得したり、不正に使用・開示した場合には不正競争防止法（平成５年法律第４７号）第２１条、第２２条により刑事罰（行為者に対する１０年以下の懲役若しくは１，０００万円以下の罰金、又はその併科。法人に対する３億円以下の罰金）が科され得る。 また、第三者から個人情報（政令第２条第２号に規定するものから取得した個人情報を除く。）を取得する場合（法第２３条第１項各号及び同条第４項各号に掲げる場合を除く。）には、提供元の法の遵守状況（例えば、オプトアウト、利用目的、開示手続き、問い合わせ・苦情の受付窓口をホームページに明記していることなど）を確認し、個人情報を適切に管理している者を提供元として選定するとともに、実際に個人情報を取得する際には、その都度、例えば、取得の経緯を示す契約書等の書面を点検する等により、当該個人情報の取得方法等を確認した上で、当該個人情報が適法に取得されたことが確認できない場合は、偽りその他不正の手段により取得されたものである可能性もあることから、その取得を自粛することを含め、慎重に対応することが望ましい。	2-2-2.個人情報の取得関係（法第１７条～第１８条関連） （１）適正取得（法第１７条関連） 法第１７条 （略） 個人情報取扱事業者は、偽り等の不正の手段により個人情報を取得してはならない。 なお、不正の競争の目的で、秘密として管理されている事業上有用な個人情報で公然と知られていないものを、不正に取得したり、不正に使用・開示した場合には不正競争防止法（平成５年法律第４７号）第２１条、第２２条により刑事罰（行為者に対する１０年以下の懲役若しくは１，０００万円以下の罰金、又はその併科。法人に対する３億円以下の罰金）が科され得る。
2-2-3-2.安全管理措置（法第２０条関連） 法第２０条	2-2-3-2.安全管理措置（法第２０条関連） 法第２０条

（略） 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、組織的、人的、物理的及び技術的な安全管理措置を講じなければならない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の程度を考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとする。その際には、特に、中小企業者（中小企業基本法（昭和３８年法律第１５４号）第２条第１項各号に掲げる中小企業者をいう。以下同じ。）においては、事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。また、個人データを記録した媒体の性質に応じた安全管理措置を講じることが望ましい。なお、クレジットカード情報については、別添の「クレジットカード情報を含む個人情報の取扱いについて」に掲げられた措置を講じることが望ましい。	（略） 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、組織的、人的、物理的及び技術的な安全管理措置を講じなければならない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、本人の個人データが漏えい、滅失又はき損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し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとする。その際には、個人データを記録した媒体の性質に応じた安全管理措置を講じることが望ましい。なお、クレジットカード情報については、別添の「クレジットカード情報を含む個人情報の取扱いについて」に掲げられた措置を講じることが望ましい。
組織的安全管理措置 組織的安全管理措置とは、安全管理について従業者（法第２１条参照）の責任と権限を明確に定め、安全管理に対する規程や手順書（以下「規程等」という。）を整備運用し、その実施状況を確認することをいう。	組織的安全管理措置 組織的安全管理措置とは、安全管理について従業者（法第２１条参照）の責任と権限を明確に定め、安全管理に対する規程や手順書（以下「規程等」という。）を整備運用し、その実施状況を確認することをいう。
【各項目を実践するために講じることが望まれる手法の例示】 ①　「個人データの安全管理措置を講じるための組織体制の整備」を実践するために講じることが望まれる手法の例示 ・従業者の役割・責任の明確化 ＊個人データの安全管理に関する従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定めることが望ましい。 ・個人データの安全管理の実施及び運用に関する責任及び権限を有する者として、個人情報保護管理者（いわゆる、チーフ・プライバシー・オフィサー（ＣＰＯ））を設置し、原則として、役員を任命すること ・個人データの取扱いを総括する専門部署の設置、及び個人情報保護管理者（ＣＰＯ）が代表者となり、社内の個人データの取扱いを監督する「管理委員会」の設置	**【各項目を実践するために講じることが望まれる手法の例示】** ①「個人データの安全管理措置を講じるための組織体制の整備」を実践するために講じることが望まれる手法の例示 ・従業者の役割・責任の明確化 ＊個人データの安全管理に関する従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定めることが望ましい。 ・個人情報保護管理者（いわゆる、チーフ・プライバシー・オフィサー（ＣＰＯ））の設置

・個人データの取扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）における作業責任者の設置及び作業担当者の限定 ・個人データを取り扱う情報システム運用責任者の設置及び担当者（システム管理者を含む。）の限定 ・個人データの取扱いにかかわるそれぞれの部署の役割と責任の明確化 ・監査責任者の設置 ・個人情報保護対策及び最新の技術動向を踏まえた情報セキュリティ対策に十分な知見を有する者が社内の対応を確認すること（必要に応じ、外部の知見を有する者を活用し確認することを含む）などによる、監査実施体制の整備 ・個人データの取扱いに関する規程等に違反している事実又は兆候があることに気づいた場合の、代表者等への報告連絡体制の整備 ・個人データの漏えい等（漏えい、滅失又はき損）の事故が発生した場合、又は発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備 ＊個人データの漏えい等についての情報は代表窓口、苦情処理窓口を通じ、外部からもたらされる場合もあるため、苦情の処理体制等との連携を図ることが望ましい（法第３１条を参照）。 ・漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備 ・漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備 ②～⑤　（略） 【個人データの取扱いに関する規程等に記載することが望まれる事項の例】 以下、(１)取得・入力、(２)移送・送信、(３)利用・加工、(４)保管・バックアップ、(５)消去・廃棄という、個人データの取扱いの流れに従い、そのそれぞれにつき規程等に記載することが望まれる事項の例を列記する。 (１) 取得・入力 ①　（略）	・個人データの取扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）における作業責任者の設置及び作業担当者の限定 ・個人データを取り扱う情報システム運用責任者の設置及び担当者（システム管理者を含む。）の限定 ・個人データの取扱いにかかわるそれぞれの部署の役割と責任の明確化 ・監査責任者の設置 ・監査実施体制の整備 ・個人データの取扱いに関する規程等に違反している事実又は兆候があることに気づいた場合の、代表者等への報告連絡体制の整備 ・個人データの漏えい等（漏えい、滅失又はき損）の事故が発生した場合、又は発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備 ＊個人データの漏えい等についての情報は代表窓口、苦情処理窓口を通じ、外部からもたらされる場合もあるため、苦情の処理体制等との連携を図ることが望ましい（法第３１条を参照）。 ・漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備 ・漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備 ②～⑤　（略） 【個人データの取扱いに関する規程等に記載することが望まれる事項の例】 以下、(１)取得・入力、(２)移送・送信、(３)利用・加工、(４)保管・バックアップ、(５)消去・廃棄という、個人データの取扱いの流れに従い、そのそれぞれにつき規程等に記載することが望まれる事項の例を列記する。 (１) 取得・入力 ①　（略）

②手続の明確化と手続に従った実施 ・(略) ・個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定（例えば、個人データを入力できる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにするとともに、スマートフォン、パソコン等の記録機能を有する機器の接続を制限し、媒体及び機器の更新に対応する。）	②手続の明確化と手続に従った実施 ・(略) ・個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定（例えば、個人データを入力できる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにする。）
（２）　(略)	（２）　(略)
(３)利用・加工 ①　(略)	(３)利用・加工 ①　(略)
②　続の明確化と手続に従った実施 ・（略） ・個人データを利用・加工できる端末に付与する機能の、業務上の必要性に基づく、限定（例えば、個人データを閲覧だけできる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにするとともに、スマートフォン、パソコン等の記録機能を有する機器の接続を制限し、媒体及び機器の更新に対応する。）	②　手続の明確化と手続に従った実施 ・（略） ・個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定（例えば、個人データを閲覧だけできる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにする。）
③・④　(略)	③・④　(略)
（４）・（５）　(略)	（４）・（５）　(略)
人的安全管理措置 人的安全管理措置とは、従業者（「個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。）に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。	人的安全管理措置 人的安全管理措置とは、従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。
物理的安全管理措置 物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の	物理的安全管理措置 物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の

防止等の措置をいう。 【物理的安全管理措置として講じなければならない事項】 ①入退館（室）管理の実施 ②盗難等の防止 ③機器・装置等の物理的な保護 【各項目を実践するために講じることが望まれる手法の例示】 ①　「入退館（室）管理」を実践するために講じることが望まれる手法の例示 ・入退館（室）の記録の保存 ②「盗難等の防止」を実践するために講じることが望まれる手法の例示 ・個人データを記した書類、媒体、携帯可能なコンピュータ等の机上及び車内等への放置の禁止 ・離席時のパスワード付きスクリーンセイバ等の起動によるのぞき見等の防止 ・個人データを含む媒体の施錠保管 ・氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管 ・個人データを取り扱う情報システムの操作マニュアルの机上等への放置の禁止 ・入退館（室）の際における業務上許可を得ていない記録機能を持つ媒体及び機器の持ち込み及び持ち出しの禁止と検査の実施 ・カメラによる撮影や作業への立ち会い等による記録又はモニタリングの実施 ③（略） 技術的安全管理措置 技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいう。	防止等の措置をいう。 【物理的安全管理措置として講じなければならない事項】 ①入退館（室）管理の実施 ②盗難等の防止 ③機器・装置等の物理的な保護 【各項目を実践するために講じることが望まれる手法の例示】 ①　「入退館（室）管理」を実践するために講じることが望まれる手法の例示 （追加） ②「盗難等の防止」を実践するために講じることが望まれる手法の例示 ・個人データを記した書類、媒体、携帯可能なコンピュータ等の机上及び車内等への放置の禁止 ・離席時のパスワード付きスクリーンセイバ等の起動によるのぞき見等の防止 ・個人データを含む媒体の施錠保管 ・氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管 ・個人データを取り扱う情報システムの操作マニュアルの机上等への放置の禁止 ③（略） 技術的安全管理措置 技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいう。

【技術的安全管理措置として講じなければならない事項】 ①個人データへのアクセスにおける識別と認証 ②個人データへのアクセス制御 ③個人データへのアクセス権限の管理 ④個人データのアクセスの記録 ⑤個人データを取り扱う情報システムについての不正ソフトウェア対策 ⑥個人データの移送・送信時の対策 ⑦個人データを取り扱う情報システムの動作確認時の対策 ⑧個人データを取り扱う情報システムの監視	【技術的安全管理措置として講じなければならない事項】 ①個人データへのアクセスにおける識別と認証 ②個人データへのアクセス制御 ③個人データへのアクセス権限の管理 ④個人データのアクセスの記録 ⑤個人データを取り扱う情報システムについての不正ソフトウェア対策 ⑥個人データの移送・送信時の対策 ⑦個人データを取り扱う情報システムの動作確認時の対策 ⑧個人データを取り扱う情報システムの監視
【各項目を実践するために講じることが望まれる手法の例示】	【各項目を実践するために講じることが望まれる手法の例示】
④「個人データへのアクセスの記録」を実践するために講じることが望まれる手法の例示 ・個人データへのアクセスや操作の成功と失敗の記録及び不正が疑われる異常な記録の存否の定期的な確認	④「個人データへのアクセスの記録」を実践するために講じることが望まれる手法の例示 ・個人データへのアクセスや操作の成功と失敗の記録
⑧「個人データを取り扱う情報システムの監視」を実践するために講じることが望まれる手法の例示 ・個人データを取り扱う情報システムの使用状況の定期的な監視 ・個人データへのアクセス状況（操作内容も含む。）の監視 ＊個人データを取り扱う情報システムを監視した結果の記録が個人情報に該当する場合があることに留意する。 ＊特権ユーザーによる個人データへのアクセス状況については、特に注意して監視することが望ましい。 ・個人データを取り扱う情報システムへの外部からのアクセス状況の監視（例えば、ＩＤＳ・ＩＰＳ等） ＊監視システムを利用する場合には、事業者等が業務で行う送受信の実態に合わせ、当該装置について適切に設定し、定期的にその動作を確認することが必要になる。	⑧「個人データを取り扱う情報システムの監視」を実践するために講じることが望まれる手法の例示 ・個人データを取り扱う情報システムの使用状況の定期的な監視 ・個人データへのアクセス状況（操作内容も含む。）の監視 ＊個人データを取り扱う情報システムを監視した結果の記録が個人情報に該当する場合があることに留意する。 ＊特権ユーザーによる個人データへのアクセス状況については、特に注意して監視することが望ましい。 ・個人データを取り扱う情報システムへの外部からのアクセス状況の監視（例えば、ＩＤＳ・ＩＰＳ等） ＊ＩＤＳ・ＩＰＳを利用する場合には、事業者等が業務で行う送受信の実態に合わせ、当該装置について適切な設定をすることが必要になる。
2-2-3-3. 従業者の監督（法第２１条関連）	2-2-3-3. 従業者の監督（法第２１条関連）

法第２１条 （略）	法第２１条 （略）
個人情報取扱事業者は、法第２０条に基づく安全管理措置を遵守させるよう、従業者に対し必要かつ適切な監督をしなければならない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、本人の個人データが漏えい、滅失又はき損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し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとする。また、特に、中小企業者においては、事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。	個人情報取扱事業者は、法第２０条に基づく安全管理措置を遵守させるよう、従業者に対し必要かつ適切な監督をしなければならない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、本人の個人データが漏えい、滅失又はき損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し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとする。
2-2-3-4.委託先の監督（法第２２条関連）	2-2-3-4.委託先の監督（法第２２条関連）
法第２２条 （略）	法第２２条 （略）
個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合、法第２０条に基づく安全管理措置を遵守させるよう、委託を受けた者に対し必要かつ適切な監督をしなければならない(2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、委託する業務内容に対して必要のない個人データを提供しないようにすることは当然のこととして、特に、中小企業者においては、自ら又は委託先の事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。 「必要かつ適切な監督」には、委託先を適切に選定すること、委託先に法第２０条に基づく安全管理措置を遵守させるために必要な契約を締結すること、委託先における委託された個人データの取扱状況を把握することが含まれる。 なお、優越的地位にある者が委託元の場合、委託元は、委託先との責任分担を無視して、本人からの損害賠償請求に係る責務を一方的に委託先に課す、委託先からの報告や監査において過度な負担を強いるなど、委託先に不当な負担を課すことがあってはならない。	個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合、法第２０条に基づく安全管理措置を遵守させるよう、委託を受けた者に対し必要かつ適切な監督をしなければならない(2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、委託する業務内容に対して必要のない個人データを提供しないようにすることは当然のこととして、取扱いを委託する個人データの内容を踏まえ、本人の個人データが漏えい、滅失又はき損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し、事業の性質及び個人データの取扱状況等に起因するリスクに応じた、必要かつ適切な措置を講じるものとする。 「必要かつ適切な監督」には、委託先を適切に選定すること、委託先に法第２０条に基づく安全管理措置を遵守させるために必要な契約を締結すること、委託先における委託された個人データの取扱状況を把握することが含まれる。
① 委託先の選定	①委託先の選定

委託先の選定に当たっては、委託先の安全管理措置が、少なくとも法第２０条で求められるものと同等であることを確認するため、以下の項目が、委託する業務内容に沿って、確実に実施されることについて、委託先の社内体制、規程等の確認、必要に応じて、実地検査等を行った上で、個人情報保護管理者（ＣＰＯ）等が、適切に評価することが望ましい。 （ア）組織的安全管理措置 ・ 個人データの安全管理措置を講じるための組織体制の整備 ・ 個人データの安全管理措置を定める規程等の整備と規程等に従った運用 ・ 個人データの取扱状況を一覧できる手段の整備 ・ 個人データの安全管理措置の評価、見直し及び改善 ・ 事故又は違反への対処 （イ）人的安全管理措置 ・ 雇用契約時における従業者との非開示契約の締結、及び委託契約等（派遣契約を含む。）における委託元と委託先間での非開示契約の締結 ・ 従業者に対する内部規程等の周知・教育・訓練の実施 （ウ）物理的安全管理措置 ・ 入退館（室）管理の実施 ・ 盗難等の防止 ・ 機器・装置等の物理的な保護 （エ）技術的安全管理措置 ・ 個人データへのアクセスにおける識別と認証 ・ 個人データへのアクセス制御 ・ 個人データへのアクセス権限の管理 ・ 個人データのアクセスの記録 ・ 個人データを取り扱う情報システムについての不正ソフトウェア対策 ・ 個人データの移送・送信時の対策 ・ 個人データを取り扱う情報システムの動作確認時の対策 ・ 個人データを取り扱う情報システムの監視 ②　委託契約の締結 委託契約には、当該個人データの取扱いに関する、必要かつ適切な安全管理措置として、委託元、委託先双方が同意した内容とともに、	委託先を適切に選定するためには、委託先において実施される個人データの安全管理措置が、委託する当該業務内容に応じて、少なくとも法第２０条で求められる安全管理措置と同等であることを、合理的に確認することが望ましい。また、委託先の評価は適宜実施することが望ましい。 ② 委託契約の締結 委託契約には、当該個人データの取扱いに関する、必要かつ適切な安全管理措置として、委託元、委託先双方が同意した内容とともに、

委託先における委託された個人データの取扱状況を合理的に把握することを盛り込むことが望ましい。 （削除）	委託先における委託された個人データの取扱状況を合理的に把握することを盛り込むことが望ましい。 なお、本人からの損害賠償請求に係る責務を、安全管理措置に係る責任分担を無視して一方的に委託先に課すなど、優越的地位にある者が委託元の場合、委託先に不当な負担を課すことがあってはならない。
③　委託先における個人データ取扱状況の把握 委託先における委託された個人データの取扱状況を把握するためには、定期的に（少なくとも年１回）、監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、個人情報保護管理者（ＣＰＯ）等が、委託の内容等の見直しを検討することを含め、適切に評価することが望ましい。	③委託先における個人データ取扱状況の把握 委託先における委託された個人データの取扱状況を把握するためには、委託契約で盛り込んだ内容の実施の程度を相互に確認することが望ましい。
委託元が委託先について「必要かつ適切な監督」を行っていない場合で、委託先が再委託をした際に、再委託先が適切といえない取扱いを行ったことにより、何らかの問題が生じたときは、元の委託元がその責めを負うことがあり得るので、再委託する場合は、注意を要する。このため、委託先が再委託を行おうとする場合は、委託を行う場合と同様、委託元は、委託先が再委託する相手方、再委託する業務内容及び再委託先の個人情報の扱い方法等について、委託先から事前報告又は承認を求める、及び委託先を通じて又は必要に応じて自らが、定期的に監査を実施する等により、委託先が再委託先に対して本条の委託先の監督を適切に果たすこと、及び再委託先が法第２０条に基づく安全管理措置を講ずることを十分に確認することが望ましい。再委託先が再々委託を行う場合以降も、再委託を行う場合と同様とする。	委託元が委託先について「必要かつ適切な監督」を行っていない場合で、委託先が再委託をした際に、再委託先が適切といえない取扱いを行ったことにより、何らかの問題が生じたときは、元の委託元がその責めを負うことがあり得るので、再委託する場合は、注意を要する。
なお、漏えいした場合に二次被害が発生する可能性が高い個人データ（例えば、クレジットカード情報（カード番号、有効期限等）を含む個人データ等）の取扱いを委託する場合は、より高い水準において「必要かつ適切な監督」を行うことが望ましい。 また、消費者等、本人の権利利益保護の観点から、事業内容の特性、規模及び実態に応じ、委託の有無、委託する事務の内容を明らかにする等、委託処理の透明化を進めることが望ましい。	なお、漏えいした場合に二次被害が発生する可能性が高い個人データ（例えば、クレジットカード情報（カード番号、有効期限等）を含む個人データ等）の取扱いを委託する場合は、より高い水準において「必要かつ適切な監督」を行うことが望ましい。 また、消費者等、本人の権利利益保護の観点から、事業内容の特性、規模及び実態に応じ、委託の有無、委託する事務の内容を明らかにする等、委託処理の透明化を進めることが望ましい。
【個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項】 ・委託元及び委託先の責任の明確化	【個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項】 ・委託元及び委託先の責任の明確化

・委託先において、個人データを取り扱う者（委託先で作業する委託先の従業者以外の者を含む）の氏名又は役職等（なお、委託の実態に応じて、例えば、契約書とは別に、個人データを取り扱う者のリスト等により、個人データを取り扱う者を把握するなど、適切な対応を行うことが望ましい。）	
・個人データの安全管理に関する事項 ・個人データの漏えい防止、盗用禁止に関する事項 ・委託契約範囲外の加工、利用の禁止 ・委託契約範囲外の複写、複製の禁止 ・委託契約期間 ・委託契約終了後の個人データの返還・消去・廃棄に関する事項	・個人データの安全管理に関する事項 ・個人データの漏えい防止、盗用禁止に関する事項 ・委託契約範囲外の加工、利用の禁止 ・委託契約範囲外の複写、複製の禁止 ・委託契約期間 ・委託契約終了後の個人データの返還・消去・廃棄に関する事項
・再委託に関する事項 ・再委託を行うに当たっての委託元への文書による事前報告又は承認	・再委託に関する事項 ・再委託を行うに当たっての委託元への文書による報告
・個人データの取扱状況に関する委託元への報告の内容及び頻度	・個人データの取扱状況に関する委託元への報告の内容及び頻度
・契約内容が遵守されていることの確認（例えば、情報セキュリティ監査なども含まれる。）	・契約内容が遵守されていることの確認（例えば、情報セキュリティ監査なども含まれる。）
・契約内容が遵守されなかった場合の措置（例えば、安全管理に関する事項が遵守されずに個人データが漏えいした場合の損害賠償に関する事項も含まれる。）	・契約内容が遵守されなかった場合の措置
・セキュリティ事件・事故が発生した場合の報告・連絡に関する事項	・セキュリティ事件・事故が発生した場合の報告・連絡に関する事項
５．個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・規格 （１）個人情報保護のためのマネジメント体制の確立 個人情報取扱事業者は、その事業規模及び活動に応じて、個人情報の保護のためのマネジメントシステムを確立し、実施し、維持し及び改善を行うことが望ましい。 なお、その体制の整備に当たっては、日本工業規格 JIS Q 15001「個人情報保護マネジメントシステム－要求事項」を、個人データの安全管理措置の実施に当たっては、日本工業規格 JIS X 5070「セキュリティ技術－情報技術セキュリティの評価基準」、日本工業規格 JIS Q 27001「情報技術－セキュリティ技術－情報セキュリティマネジメントシステム―要求事項」、日本工業規格 JIS Q 27002「情報技術―セキュリティ技術―情報セキュリティマネジメントの実践のための規範 」、独立行政法人情報	**５．個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・規格** （１）個人情報保護のためのマネジメント体制の確立 個人情報取扱事業者は、その事業規模及び活動に応じて、個人情報の保護のためのマネジメントシステムを確立し実施し、維持し及び改善を行うことが望ましい。 なお、その体制の整備に当たっては、日本工業規格 JIS Q 15001「個人情報保護マネジメントシステム－要求事項」を、個人データの安全管理措置の実施に当たっては、日本工業規格 JIS X 5070「セキュリティ技術－情報技術セキュリティの評価基準」、日本工業規格 JIS Q 27001「情報技術－セキュリティ技術－情報セキュリティマネジメントシステム―要求事項」、日本工業規格 JIS Q 27002「情報技術―セキュリティ技術―情報セキュリティマネジメントの実践のための規範 」、ＣＲＹＰＴＲＥＣ

処理推進機構の「組織における内部不正防止ガイドライン」、総務省・経済産業省の「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（ＣＲＹＰＴＲＥＣ暗号リスト）」、ISO/IEC 18033（暗号アルゴリズム国際規格）等を、個人データの安全管理措置の実施状況の確認に当たっては、経済産業省の「情報セキュリティ監査制度」を、それぞれ参考にすることができる。	（暗号技術評価プロジェクト）の「電子政府推奨暗号リスト」、ISO/IEC 18033（暗号アルゴリズム国際規格）等を、個人データの安全管理措置の実施状況の確認に当たっては、経済産業省の「情報セキュリティ監査制度」を、それぞれ参考にすることができる。