「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
2-2-3-2.安全管理措置（法第２０条関連） 法第２０条 （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 **【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】** ※技術的安全管理措置については、①から⑧までの各項目を遵守するとともに、複数の手法を組み合わせ、個人データ及びそれを取り扱う情報システム全体の安全性を確保することが重要である。各項目を実践するための各手法については、以降の①～⑧において、項目ごとに例示する。また、技術的安全管理措置の典型的な手法には例えば次のような方法がある。 「②個人データへのアクセス制御」 典型的手法）ファイアウォール、ルータ等の設定 「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	2-2-3-2.安全管理措置（法第２０条関連） 法第２０条 （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 **【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】**

対策」 典型的手法）ウイルス対策ソフトウェアの導入	
①「個人データへのアクセスにおける識別と認証」を実践するために講じることが望まれる手法の例示 ・個人データに対する正当なアクセスであることを確認するために正当なアクセス権限を有する者であることの識別と認証（例えば、IDとパスワードによる認証、ワンタイムパスワードによる認証、物理的に所持が必要な認証デバイス（ＩＣカード等）による認証、生体認証等）の実施 ＊識別と認証は、複数の手法を組み合わせて実現することが望ましい。 ＊ID とパスワードを利用する場合には、パスワードの有効期限の設定、同一又は類似パスワードの再利用の制限、最低パスワード文字数の設定、一定回数以上ログインに失敗した ID を停止する等の措置を講じることが望ましい。 ＊生体認証を利用する場合には、当該識別と認証の方法を実施するために必要な情報が本人と切り離し不可能な個人情報に該当する場合があることに留意する。 ・個人データへのアクセス権限を有する者が使用できる端末又はアドレス等の識別と認証（例えば、MAC アドレス認証、IP アドレス認証、電子証明書等）の実施	①「個人データへのアクセスにおける識別と認証」を実践するために講じることが望まれる手法の例示 ・個人データに対する正当なアクセスであることを確認するために正当なアクセス権限を有する者であることの識別と認証（例えば、IDとパスワードによる認証、生体認証等）の実施 ＊ID とパスワードを利用する場合には、パスワードの有効期限の設定、同一又は類似パスワードの再利用の制限、最低パスワード文字数の設定、一定回数以上ログインに失敗した ID を停止する等の措置を講じることが望ましい。 ・個人データへのアクセス権限を有する者が使用できる端末又はアドレス等の識別と認証（例えば、MAC アドレス認証、IP アドレス認証、電子証明書や秘密分散技術を用いた認証等）の実施
②「個人データへのアクセス制御」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権限を付与すべき者の最小化 ・識別に基づいたアクセス制御（パスワード設定をしたファイルがだれでもアクセスできる状態は、アクセス制御はされているが、識別がされていないことになる。このような場合には、パスワードを知っている者が特定され、かつ、アクセスを許可する者に変更があるたびに、適切にパスワードを変更する必要がある。）の実施 ・アクセス権限を有する者に付与する権限の最小化 ・個人データを格納した情報システムへの同時利用者数の制限 ・個人データを格納した情報システムの利用時間の制限（例えば、休業日や業務時間外等の時間帯には情報システムにアクセスできない	②「個人データへのアクセス制御」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権限を付与すべき者の最小化 ・識別に基づいたアクセス制御（パスワード設定をしたファイルがだれでもアクセスできる状態は、アクセス制御はされているが、識別がされていないことになる。このような場合には、パスワードを知っている者が特定され、かつ、アクセスを許可する者に変更があるたびに、適切にパスワードを変更する必要がある。）の実施 ・アクセス権限を有する者に付与する権限の最小化 ・個人データを格納した情報システムへの同時利用者数の制限 ・個人データを格納した情報システムの利用時間の制限（例えば、休業日や業務時間外等の時間帯には情報システムにアクセスできない

ようにする等） ・個人データを格納した情報システムへの無権限アクセスからの保護（例えば、ファイアウォール、ルータ等の設定） ＊個人データを格納するためのデータベースを構成要素に含む情報システムを構築する場合には、当該情報システム自体へのアクセス制御に加えて、情報システムの構成要素であるデータベースへのアクセス制御を別に実施し、それぞれにアクセス権限を設定することが望ましい。 ＊アクセス権限の設定を情報システム全体と別に実施する場合にあっては、無権限アクセスからの保護に係る機器等の設定として、特に不要アカウントの無効化や標準アカウントのパスワード変更を実施することが望ましい。 ・個人データにアクセス可能なアプリケーションの無権限利用の防止（例えば、アプリケーションシステムに認証システムを実装する、業務上必要となる者が利用するコンピュータのみに必要なアプリケーションシステムをインストールする、業務上必要な機能のみメニューに表示させる等） ＊情報システムの特権ユーザーであっても、情報システムの管理上個人データの内容を知らなくてもよいのであれば、個人データへ直接アクセスできないようにアクセス制御をすることが望ましい。 ＊特権ユーザーに対するアクセス制御については、例えば、トラステッドＯＳやセキュアＯＳ、アクセス制御機能を実現する製品等の利用が考えられる。 ・個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証（例えば、ＯＳ・ウェブアプリケーションのぜい弱性有無の検証） ③「個人データへのアクセス権限の管理」を実践するために講じることが望まれる手法の例示 ・個人データにアクセスできる者を許可する権限管理の適切かつ定期的な実施（例えば、定期的に個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする。） ＊個人データにアクセスできる者を許可する権限については、情報	ようにする等） ・個人データを格納した情報システムへの無権限アクセスからの保護（例えば、ファイアウォール、ルータ等の設定） ・個人データにアクセス可能なアプリケーションの無権限利用の防止（例えば、アプリケーションシステムに認証システムを実装する、業務上必要となる者が利用するコンピュータのみに必要なアプリケーションシステムをインストールする、業務上必要な機能のみメニューに表示させる等） ＊情報システムの特権ユーザーであっても、情報システムの管理上個人データの内容を知らなくてもよいのであれば、個人データへ直接アクセスできないようにアクセス制御をすることが望ましい。 ＊特権ユーザーに対するアクセス制御については、例えば、トラステッドＯＳやセキュアＯＳ、アクセス制御機能を実現する製品等の利用が考えられる。 ・個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証（例えば、ウェブアプリケーションのぜい弱性有無の検証） ③「個人データへのアクセス権限の管理」を実践するために講じることが望まれる手法の例示 ・個人データにアクセスできる者を許可する権限管理の適切かつ定期的な実施（例えば、定期的に個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする。）

システム内において当該権限を含む管理者権限を分割する等して、不正利用を防止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必要最小限のアクセス制御の実施	・個人データを取り扱う情報システムへの必要最小限のアクセス制御の実施
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 ＊個人データへのアクセスや操作の成功と失敗の記録については、情報システムを構成する各システムへのアクセスや操作の成功と失敗等の記録を組み合わせ、各個人データへのアクセスや操作の失敗を全体として記録することが考えられる。	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（例えば、個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録）
・採取した記録の漏えい、滅失及びき損からの適切な保護 ＊採取した記録を漏えい、滅失及びき損から保護するためには、当該記録を適切に管理された外部記録媒体ないしログ収集用のサーバー等に速やかに移動することが望ましい。 ＊システム管理者等の特権ユーザーのアクセス権限を用いても、採取した記録を改ざん・消去できないよう、保全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。	・採取した記録の漏えい、滅失及びき損からの適切な保護 ＊個人データを取り扱う情報システム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。
⑤「個人データを取り扱う情報システムについて不正ソフトウェア対策」を実践するために講じることが望まれる手法の例示 ・ウイルス対策ソフトウェアの導入及び当該ソフトウェアの有効性・安定性の確認（例えば、パターンファイルや修正ソフトウェアの更新の確認） ・端末及びサーバー等のオペレーティングシステム（ＯＳ）、ミドルウェア（ＤＢＭＳ等）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用 ・組織で許可していないソフトウェアの導入防止のための対策	⑤「個人データを取り扱う情報システムについて不正ソフトウェア対策」を実践するために講じることが望まれる手法の例示 ・ウイルス対策ソフトウェアの導入 ・オペレーティングシステム（ＯＳ）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用 ・不正ソフトウェア対策の有効性・安定性の確認（例えば、パターンファイルや修正ソフトウェアの更新の確認）
⑥「個人データの移送（運搬、郵送、宅配便等）・送信時の対策」を実践するために講じることが望まれる手法の例示	⑥「個人データの移送（運搬、郵送、宅配便等）・送信時の対策」を実践するために講じることが望まれる手法の例示

・個人データの移送時における紛失・盗難に備えるための対策（例えば、媒体に保管されている個人データの暗号化等の秘匿化） ・盗聴される可能性のあるネットワーク（例えば、インターネットや無線ＬＡＮ等）による個人データの送信（例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）時における、個人データの暗号化等の秘匿化（例えば、ＳＳＬ、Ｓ／ＭＩＭＥ等） ＊暗号を利用する場合には、復号に必要な鍵についても十分注意して管理する必要がある。	・移送時における紛失・盗難が生じた際の対策（例えば、媒体に保管されている個人データの暗号化等の秘匿化） ・盗聴される可能性のあるネットワーク（例えば、インターネットや無線ＬＡＮ等）で個人データを送信（例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）する際の、個人データの暗号化等の秘匿化
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」を実践するために講じることが望まれる手法の例示 ・情報システムの動作確認時のテストデータとして個人データを利用することの禁止（正確な動作確認を要する等、個人データの利用が不可欠な場合であっても、動作確認に影響のない範囲で、個人データの一部を他のデータに置き換える等の措置を講じることが考えられる。） ・情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれないことの検証	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」を実践するために講じることが望まれる手法の例示 ・情報システムの動作確認時のテストデータとして個人データを利用することの禁止 ・情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれないことの検証
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。	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。

2-2-4.第三者への提供（法第２３条関連） （1）～（2）（略） （3）第三者に該当しないもの（法第２３条第４項関連） 以下の（ⅰ）から（ⅲ）までの場合については、個人情報取扱事業者とは別の主体として形式的には第三者に該当するものの、本人との関係において提供主体である個人情報取扱事業者と一体のものとして取り扱うことに合理性がある場合には、第三者に該当しないものとすべきとの考え方に基づき、第三者に該当しないとしており、このような要件を満たす場合には、本人の同意又は第三者提供におけるオプトアウトを行うことなく、情報の提供を行うことができる。 （ⅰ）～（ⅱ）（略） （ⅲ）共同利用（法第２３条第４項第３号関連） 法第２３条第４項第３号 （略） 個人データを特定の者との間で共同して利用する場合であって、以下の①から④までの情報をあらかじめ※1本人に通知※2し、又は本人が容易に知り得る状態※3に置いておくとともに、共同して利用することを明らかにしているときには、当該個人データの提供を受ける事業者は、本人から見て、当該個人データを提供する事業者と一体のものとして取り扱われることに合理性があると考えられることから、第三者に該当しない。また、既に特定の事業者が取得している個人データを他の事業者と共同して利用する場合には、既に取得している事業者が法第１５条第１項の規定により特定した利用目的の範囲で共同して利用しなければならない。 また、事業者が共同利用を実施する場合には、共同利用者における責任等を明確にし円滑に実施する観点から、①から④までの情報のほか、以下〇ページに掲げる（ア）から（カ）までの事項について、あらかじめ取り決めておくことが望ましい。	2-2-4.第三者への提供（法第２３条関連） （1）～（2）（略） （3）第三者に該当しないもの（法第２３条第４項関連） 以下の（ⅰ）から（ⅲ）までの場合は、第三者に該当しないため、本人の同意又は第三者提供におけるオプトアウトを行うことなく、情報の提供を行うことができる。 （ⅰ）～（ⅱ）（略） （ⅲ）共同利用（法第２３条第４項第３号関連） 法第２３条第４項第３号 （略） 個人データを特定の者との間で共同して利用する場合、以下の①から④までの情報をあらかじめ※1本人に通知※2し、又は本人が容易に知り得る状態※3に置いておくとともに、共同して利用することを明らかにしている場合は、第三者に該当しない。また、既に特定の事業者が取得している個人データを他の事業者と共同して利用する場合は、既に取得している事業者が法第１５条第１項の規定により特定した利用目的の範囲で共同して利用しなければならない。 共同利用する場合、①から④までの情報のほか、あらかじめ一定の事項につき取り決めておくことが望ましい。

共同利用の対象となる個人データの提供については、必ずしもすべての共同利用者が双方向で行う必要はなく、一部の共同利用者に対し、一方向で行うこともできる。 個人データの管理について責任を有する者は、利用目的の達成に必要な範囲内において、共同利用者間で利用している個人データを正確かつ最新の内容に保つよう努めなければならない。 なお、共同利用か委託かは、個人データの取扱いの形態によって判断されるものであって、共同利用者の範囲に委託先事業者が含まれる場合であっても、委託先との関係は、共同利用となるわけではなく、委託先の監督義務を免れるわけでもない。 例えば、グループ企業でイベントを開催する場合において、各子会社から親会社（幹事会社）に顧客情報を集めた上で展示会の案内を発送するときには共同利用となるが、自社でイベントを開催する場合において、案内状を発送するために発送代行事業者に顧客情報を提供するときには、共同利用者の範囲に含まれるグループ企業内の事業者への提供であったとしても、委託であって、共同利用とはならない。 ※１「あらかじめ」とは、「個人データの共同利用に当たりあらかじめ」をいう。 ※２「本人に通知」については、2-1-7. 参照。 ※３「本人が容易に知り得る状態」については、2-1-11. 参照。 **【共同利用を行うことがある事例】** 事例１）グループ企業で総合的なサービスを提供するために取得時の利用目的（法第１５条第２項の規定に従い変更された利用目的を含む。以下同じ。）の範囲内で情報を共同利用する場合 事例２）親子兄弟会社の間で取得時の利用目的の範囲内で個人データを共同利用する場合 事例３）外国の会社と取得時の利用目的の範囲内で個人データを共同利用する場合 事例４）企業ポイント等を通じた連携サービスを提供する提携企業の間で取得時の利用目的の範囲内で個人データを共同利用する場合 **①共同して利用される個人データの項目**	共同利用の対象となる個人データの提供については、必ずしもすべての共同利用者が双方向で行う必要はなく、一部の共同利用者に対し、一方向で行うこともできる。 個人データの管理について責任を有する者は、利用目的の達成に必要な範囲内において、共同利用者間で利用している個人データを正確かつ最新の内容に保つよう努めなければならない。 なお、共同利用か委託かは、個人データの取扱いの形態によって判断されるものであって、共同利用者の範囲に委託先事業者が含まれる場合であっても、委託先との関係は、共同利用となるわけではなく、委託先の監督義務を免れるわけでもない。 例えば、グループ企業でイベントを開催する場合に、各子会社から親会社（幹事会社）に顧客情報を集めた上で展示会の案内を発送する場合は共同利用となるが、自社でイベントを開催する場合に、案内状を発送するために発送代行事業者に顧客情報を提供する場合は、共同利用者の範囲に含まれるグループ企業内の事業者への提供であったとしても、委託であって、共同利用とはならない。 ※１「あらかじめ」とは、「個人データの共同利用に当たりあらかじめ」をいう。 ※２「本人に通知」については、2-1-7. 参照。 ※３「本人が容易に知り得る状態」については、2-1-11. 参照。 **【共同利用を行うことがある事例】** 事例１）グループ企業で総合的なサービスを提供するために取得時の利用目的（法第１５条第２項の規定に従い変更された利用目的を含む。以下同じ。）の範囲内で情報を共同利用する場合 事例２）親子兄弟会社の間で取得時の利用目的の範囲内で個人データを共同利用する場合 事例３）外国の会社と取得時の利用目的の範囲内で個人データを共同利用する場合 事例４）企業ポイント等を通じた連携サービスを提供する提携企業の間で取得時の利用目的の範囲内で個人データを共同利用する場合 **①共同して利用される個人データの項目**

個人データの項目について、本人に通知し、又は本人が容易に知り得る状態に置いていなければならない。 事例１）氏名、住所、電話番号 事例２）氏名、商品購入履歴 **②共同して利用する者の範囲** 「共同利用の趣旨」は、本人から見て、当該個人データを提供する事業者と一体のものとして取り扱われることに合理性がある範囲で当該個人データを共同して利用することである。 したがって、共同利用者の範囲については、本人がどの事業者まで将来利用されるか判断できる程度に明確にする必要がある。 当該範囲が明確である限りにおいては、事業者の名称等を個別にすべて列挙する必要がない場合もある。 事例）本人がどの事業者まで利用されるか判断できる程度に明確な形で示された「提携基準」及び「最新の共同利用者のリスト」等を、共同利用者の全員が、本人が容易に知り得る状態に置いているとき **③利用する者の利用目的** 共同して利用する個人データについて、その取得時の利用目的をすべて、本人に通知し、又は本人が容易に知り得る状態に置いていなければならない。 利用目的が個人データの項目によって異なる場合には区別して記載することが望ましい。 **④当該個人データの管理について責任を有する者の氏名又は名称** 開示等の求め及び苦情を受け付け、その処理に尽力するとともに、個人データの内容等について、開示、訂正、利用停止等の権限を有し、安全管理等個人データの管理について責任を有する者の氏名又は名称について、本人に通知し、又は本人が容易に知り得る状態に置いていなければならない。 ここでいう「責任を有する者」とは、共同して利用するすべての事業者の中で、第一次的に苦情の受付・処理、開示・訂正等を行う	事例１）氏名、住所、電話番号 事例２）氏名、商品購入履歴 **②共同利用者の範囲（本人からみてその範囲が明確であることを要するが、範囲が明確である限りは、必ずしも個別列挙が必要ない場合もある。）** 事例）最新の共同利用者のリストを本人が容易に知り得る状態に置いているとき **③利用する者の取得時の利用目的（共同して利用する個人データのすべての利用目的）** **④開示等の求め及び苦情を受け付け、その処理に尽力するとともに、個人データの内容等について、開示、訂正、利用停止等の権限を有し、安全管理等個人データの管理について責任を有する者の氏名又は名称（共同利用者の中で、第一次的に苦情の受付・処理、開示・訂正等を行う権限を有する事業者を、「責任を有する者」といい、共同利用者の内部の担当責任者をいうのではない。）**

権限を有する事業者をいい、共同利用者のうち一事業者の内部の担当責任者をいうものではない。	
【上記①から④までの事項のほかに取り決めておくことが望ましい事項】 （ア）共同利用者の要件（グループ会社であること、特定のキャンペーン事業の一員であること等、共同利用による事業遂行上の一定の枠組） （イ）各共同利用者の個人情報取扱責任者、問い合わせ担当者及び連絡先 （ウ）共同利用する個人データの取扱いに関する事項 ・個人データの漏えい等防止に関する事項 ・目的外の加工、利用、複写、複製等の禁止 ・共同利用終了後のデータの返還、消去、廃棄に関する事項 （エ）共同利用する個人データの取扱いに関する取決が遵守されなかった場合の措置 （オ）共同利用する個人データに関する事件・事故が発生した場合の報告・連絡に関する事項 （カ）共同利用を終了する際の手続	**【上記①から④までの事項のほかに取り決めておくことが望ましい事項】** ●共同利用者の要件（グループ会社であること、特定のキャンペーン事業の一員であること等、共同利用による事業遂行上の一定の枠組） ●各共同利用者の個人情報取扱責任者、問い合わせ担当者及び連絡先 ●共同利用する個人データの取扱いに関する事項 ・個人データの漏えい等防止に関する事項 ・目的外の加工、利用、複写、複製等の禁止 ・共同利用終了後のデータの返還、消去、廃棄に関する事項 ●共同利用する個人データの取扱いに関する取決が遵守されなかった場合の措置 ●共同利用する個人データに関する事件・事故が発生した場合の報告・連絡に関する事項 ●共同利用を終了する際の手続
法第２３条第５項 （略）	法第２３条第５項 （略）
上記③及び④については、社会通念上、本人が想定することが困難でないと認められる範囲内※1で変更することができ、変更する前に、本人に通知※2又は本人が容易に知り得る状態※3に置かなければならない。 また、上記①及び②については原則として変更は認められないが、次の場合、引き続き共同利用を行うことができる。	上記③及び④については、社会通念上、本人が想定することが困難でないと認められる範囲内※1で変更することができ、変更する前に、本人に通知※2又は本人が容易に知り得る状態※3に置かなければならない。 また、上記①及び②については原則として変更は認められないが、次の場合、引き続き共同利用を行うことができる。
【引き続き共同利用を行うことができる事例】 事例１）共同利用を行う事業者や個人データの項目の変更につき、あらかじめ本人の同意を得た場合 事例２）共同利用を行う事業者の名称に変更があるが、当該事業者の事業内容に変更がない場合	**【引き続き共同利用を行うことができる事例】** 事例１）共同利用を行う事業者や個人データの項目の変更につき、あらかじめ本人の同意を得た場合 事例２）共同利用を行う事業者の名称に変更があるが、当該事業者の事業内容に変更がない場合

事例３）共同利用を行う事業者について事業の承継※４が行われた場合 ※１「本人が想定することが困難でないと認められる範囲内」については、2-2-1.(2)参照。 ※２「本人に通知」については、2-1-7.参照。 ※３「本人が容易に知り得る状態」については、2-1-11.参照。 ※４「事業の承継」については、2-2-4.(3)(ⅱ)参照。	事例３）共同利用を行う事業者について事業の承継※４が行われた場合 ※１「本人が想定することが困難でないと認められる範囲内」については、2-2-1.(2)参照。 ※２「本人に通知」については、2-1-7.参照。 ※３「本人が容易に知り得る状態」については、2-1-11.参照。 ※４「事業の承継」については、2-2-4.(3)(ⅱ)参照。
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ー要求事項」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「セキュリティ技術ー情報技術セキュリティの評価基準」、日本工業規格 JIS Q 27001「情報技術ーセキュリティ技術ー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（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。 （２）個人情報保護を推進する上での考え方や方針の策定等 個人情報取扱事業者は、「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、それをウェブ画面への掲載又は店舗の見やすい場所への掲示等により公表し、あらかじめ、対外的に分かりやすく説明することが、消費者等本人との信頼関係を構築し事業活動に対する社会の信頼を確保するために重要である。 個人情報取扱事業者は、一定の事項に関して公表しなければならない	**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** 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ー要求事項」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「セキュリティ技術ー情報技術セキュリティの評価基準」、日本工業規格 JIS Q 27001「情報技術ーセキュリティ技術ー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（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。 また、個人情報取扱事業者は、「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、それをウェブ画面への掲載又は店舗の見やすい場所への掲示等により公表し、あらかじめ、対外的に分かりやすく説明することが、事業活動に対する社会の信頼を確保するために重要である。 個人情報取扱事業者は、一定の事項に関して公表しなければならない

が（2-1-8 参照）、個人情報取扱事業者の個人情報保護を推進する上での考え方や方針には、消費者等本人の権利利益の保護の観点から、以下に掲げる点を考慮した事項を盛り込み、本人からの求めに一層対応していくことも重要である。	が（2-1-8 参照）、事業者の個人情報保護を推進する上での考え方や方針には、消費者等、本人の権利利益の保護の観点から、以下に掲げる点を考慮した事項を盛り込み、本人からの求めに一層対応していくことも重要である。
個人情報保護を推進する上での考え方や方針の策定等において考慮すべき事項 ●事業の内容及び規模を考慮した適切な個人情報の取扱いに関すること。 （ア）取得する個人情報の利用目的（法第１８条関係） すべての利用目的を列記するのではなく、事業内容を勘案して顧客の種類ごとに利用目的を限定して示すなど、事業内容の特性、規模及び実態に応じ、本人にとって利用目的がより明確になるようにすることが望ましい。 （イ）＜個人データの取扱いの委託を行う場合＞（法第２２条関係） 事業内容の特性、規模及び実態に応じ委託処理の透明化を進めることを盛り込むことが望ましい。 ・個人データの委託を行うこと。 ・委託する事務の内容 （ウ）＜本人の同意なく第三者提供する場合＞（法第２３条第２項及び第３項関係） ・利用目的に第三者提供が含まれていること。 ・第三者に提供される個人データの項目 ・第三者への提供の手段又は方法 ・本人の求めに応じて第三者への提供を停止すること。 （エ）＜共同利用する場合＞（法第２３条第４項及び第５項） ・特定の者との間で共同利用すること。 ・共同して利用される個人データの項目 ・共同利用者の範囲 ・共同して利用する者の利用目的 ・共同して利用する者のうち、個人データの管理について責任を有する者の氏名又は名称 （オ）以下の保有個人データに関すること（法第２４条、第２５条及び第２７条関係）。 個人情報の取得元又は取得方法（取得源の種類等）を可能な限り	●事業の内容及び規模を考慮した適切な個人情報の取扱いに関すること。 （ア）取得する個人情報の利用目的（法第１８条関係） すべての利用目的を列記するのではなく、事業内容を勘案して顧客の種類ごとに利用目的を限定して示すなど、事業内容の特性、規模及び実態に応じ、本人にとって利用目的がより明確になるようにすることが望ましい。 （イ）＜個人データの取扱いの委託を行う場合＞（法第２２条関係） 事業内容の特性、規模及び実態に応じ委託処理の透明化を進めることを盛り込むことが望ましい。 ・個人データの委託を行うこと。 ・委託する事務の内容 （ウ）＜本人の同意なく第三者提供する場合＞（法第２３条第２項及び第３項関係） ・利用目的に第三者提供が含まれていること。 ・第三者に提供される個人データの項目 ・第三者への提供の手段又は方法 ・本人の求めに応じて第三者への提供を停止すること。 （エ）＜共同利用する場合＞（法第２３条第４項及び第５項） ・特定の者との間で共同利用すること。 ・共同して利用される個人データの項目 ・共同利用者の範囲 ・共同して利用する者の利用目的 ・共同して利用する者のうち、個人データの管理について責任を有する者の氏名又は名称 （オ）以下の保有個人データに関すること（法第２４条、第２５条及び第２７条関係）。 個人情報の取得元又は取得方法（取得源の種類等）を可能な限り

具体的に明記したり、本人から求めがあった場合には、ダイレクトメールの発送停止等自主的に利用停止に応じたりするなど、事業活動の特性、規模、実態を考慮して、本人からの求めに対応していくことを盛り込むことが望ましい。 ・自己の氏名又は名称 ・すべての保有個人データの利用目的 ・「開示等の求め」に応じる手続（定めた場合に限る。） ・保有個人データの利用目的の通知及び開示に係る手数料の額（定めた場合に限る。） ・苦情の申出先（認定個人情報保護団体の対象事業者※である場合には当該認定個人情報保護団体の名称及び苦情解決の申出先を含む。） （カ）開示等の求めに応じる手続に関すること（法第２９条関係）。 ・申請書の様式（定めた場合に限る。） ・受け付ける方法（定めた場合に限る。） ・保有個人データの特定に役立つ情報の提供 （キ）問い合わせ及び苦情の受付窓口に関すること（法第２３条第５項、第２４条第１項、第２９条第１項及び第３１条関係）。 ●個人情報の保護に関する法律を遵守すること。 ●個人情報の安全管理措置に関すること。 ●マネジメントシステムの継続的改善に関すること。 ※「認定個人情報保護団体の対象事業者」とは、認定個人情報保護団体の構成員である個人情報取扱事業者（傘下企業）、又は団体が苦情処理等の業務を行うことについて当該団体と契約関係等にある事業者等 （３）消費者等本人に対する分かりやすい説明の実施 個人情報取扱事業者は、消費者等本人との信頼関係を構築する観点から、消費者等本人に対して、個人情報取扱事業者の個人情報保護を推進する上での考え方や方針等について、以下に掲げる基準を参考にして、冗長で分かりにくい表現を避け、消費者等本人に誤解を与えることなく	具体的に明記したり、本人から求めがあった場合には、ダイレクトメールの発送停止等自主的に利用停止に応じたりするなど、事業活動の特性、規模、実態を考慮して、本人からの求めに対応していくことを盛り込むことが望ましい。 ・自己の氏名又は名称 ・すべての保有個人データの利用目的 ・「開示等の求め」に応じる手続（定めた場合に限る。） ・保有個人データの利用目的の通知及び開示に係る手数料の額（定めた場合に限る。） ・苦情の申出先（認定個人情報保護団体の対象事業者※である場合には当該認定個人情報保護団体の名称及び苦情解決の申出先を含む。） （カ）開示等の求めに応じる手続に関すること（法第２９条関係）。 ・申請書の様式（定めた場合に限る。） ・受け付ける方法（定めた場合に限る。） ・保有個人データの特定に役立つ情報の提供 （キ）問い合わせ及び苦情の受付窓口に関すること（法第２３条第５項、第２４条第１項、第２９条第１項及び第３１条関係）。 ●個人情報の保護に関する法律を遵守すること。 ●個人情報の安全管理措置に関すること。 ●マネジメントシステムの継続的改善に関すること。 ※「認定個人情報保護団体の対象事業者」とは、認定個人情報保護団体の構成員である個人情報取扱事業者（傘下企業）、又は団体が苦情処理等の業務を行うことについて当該団体と契約関係等にある事業者等

分かりやすい表現で表示することが望ましい。 **分かりやすい説明の実施に際して参考とすべき基準** １．記載事項 （１）必要十分な記載事項 １　個人情報の取扱いに関する情報として、以下の 7 項目が記載されていること １）提供するサービスの概要 ２）取得する個人情報と取得の方法 ３）個人情報の利用目的 ４）個人情報や個人情報を加工したデータの第三者への提供の有無及び提供先 ５）消費者等本人による個人情報の提供の停止の可否、訂正及びその方法 ６）問合せ先 ７）保存期間、廃棄 ２．記載方法 （１）取得する個人情報とその取得方法に係る記載方法 ２　取得する個人情報の項目とその取得方法について、可能な限り細分化し、具体的に記載していること ３　取得する個人情報の項目やその取得方法のうち、消費者等本人にとって分かりにくいものを明確に記載していること （２）個人情報の利用目的に係る記載方法 ４　取得する個人情報の利用目的を特定し、具体的に記載していること ５　個人情報の利用目的が、取得する個人情報の項目と対応して記載されていること ６　取得する個人情報の利用目的のうち、消費者等本人にとって分かりにくいものを明確に記載していること （３）第三者への提供の有無及び個人情報や個人情報を加工したデータの提供先に係る記載方法 ７　個人情報取扱事業者が取得する個人情報や個人情報を加工したデータを第三者に提供する場合、その提供先（事後的に提供先を変更する場合は提供先の選定条件を含む）及び提供目的が記載されていること	

８　個人情報取扱事業者が取得した個人情報を加工したデータを第三者に提供する場合、その加工方法が記載されていること （４）消費者等本人による個人情報の提供の停止の可否及びその方法に係る記載方法 ９　消費者等本人が個人情報取扱事業者による個人情報の取得の中止又は利用の停止が可能であるかが記載され、可能である場合には取得の中止方法又は利用の停止方法を明示して記載していること 上記の「参考とすべき基準」は、個人情報を含む「パーソナルデータ」を利活用してサービスを行う事業者が、消費者から「パーソナルデータ」を取得し利用する際に、消費者に対して行う情報提供や個人情報保護を推進する上での考え方や方針等を分かりやすく説明した文書等の内容の適切性を第三者が事前に評価する際のツールとして経済産業省が策定した「評価基準」を基に作成したものである。 同評価基準の評価方法等については、経済産業省ホームページの「個人情報保護」のページ中に掲載されている。 （経済産業省ホームページの「個人情報保護」のページ） http://www.meti.go.jp/policy/it_policy/privacy/index.html	
（４）その他参考となる事項 本ガイドラインで取り上げた典型的な事例のほか、より具体的な事例は「個人情報保護ガイドライン等に関するＱ＆Ａ」で取り上げる。ただし、同Ｑ＆Ａの事例も、すべての事例を網羅することを目的とするものではなく、実際には個別事案ごとの検討が必要となる。 同Ｑ＆Ａは、経済産業省ホームページの「個人情報保護」のページ中に掲載され、随時更新する予定である。 （経済産業省ホームページの「個人情報保護」のページ） http://www.meti.go.jp/policy/it_policy/privacy/index.html	本ガイドラインで取り上げた典型的な事例のほか、より具体的な事例は「個人情報保護ガイドライン等に関するＱ＆Ａ」で取り上げる。ただし、同Ｑ＆Ａの事例も、すべての事例を網羅することを目的とするものではなく、実際には個別事案ごとの検討が必要となる。 同Ｑ＆Ａは、経済産業省ホームページの「個人情報保護」のページ中に掲載され、随時更新する予定である。 （経済産業省ホームページの「個人情報保護」のページ） http://www.meti.go.jp/policy/it_policy/privacy/index.html