

【新旧対照表】「個人情報保護指針」

(下線部分改正箇所)

旧	新	根拠法令等
<p>第1条～第11条 略</p>	<p>第1条～第11条 同左</p>	
<p>(安全管理措置)</p> <p>第12条 協会員は、その取り扱う個人データの漏えい、滅失又は毀損(以下「漏えい等」という。)の防止その他の個人データの安全管理のため、安全管理に係る基本方針・取扱規程等の整備及び安全管理措置に係る実施体制の整備等の必要かつ適切な措置を講じなければならない。必要かつ適切な措置は、個人データの取得・利用・保管等の各段階に応じた「組織的安全管理措置」、「人的安全管理措置」、「物理的安全管理措置」、「技術的安全管理措置」及び「外的環境の把握」を含むものでなければならない。</p> <p>なお、当該措置は、個人データが漏えい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、個人データの取扱状況及び個人データを記録した媒体の性質等に起因するリスクに応じたものとする。</p> <p>例えば、不特定多数者が書店で随時に購入可能な名簿で、協会員において全く加工をしていないものについては、個人の権利利益を侵害するおそれは低いと考えられることから、それを処分するために文書細断機等による処理を行わずに廃棄し、又は廃品回収に出したとしても、協会員の安全管理措置の義務違反にはならない。</p> <p>(新設)</p> <p>本条における用語の定義は、次のとおりである。</p> <p>(1)～(5) 略</p> <p>2、3 略</p>	<p>(安全管理措置)</p> <p>第12条 協会員は、その取り扱う個人データの漏えい、滅失又は毀損(以下「漏えい等」という。)の防止その他の個人データの安全管理のため、安全管理に係る基本方針・取扱規程等の整備及び安全管理措置に係る実施体制の整備等の必要かつ適切な措置を講じなければならない。必要かつ適切な措置は、個人データの取得・利用・保管等の各段階に応じた「組織的安全管理措置」、「人的安全管理措置」、「物理的安全管理措置」、「技術的安全管理措置」及び「外的環境の把握」を含むものでなければならない。</p> <p>なお、当該措置は、個人データが漏えい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、個人データの取扱状況及び個人データを記録した媒体の性質等に起因するリスクに応じたものとする。</p> <p>例えば、不特定多数者が書店で随時に購入可能な名簿で、協会員において全く加工をしていないものについては、個人の権利利益を侵害するおそれは低いと考えられることから、それを処分するために文書細断機等による処理を行わずに廃棄し、又は廃品回収に出したとしても、協会員の安全管理措置の義務違反にはならない。</p> <p><u>なお、保護法第23条における「その他の個人データの安全管理のために必要かつ適切な措置」には、協会員が取得し、又は取得しようとしている個人情報であって、当該協会員が個人データとして取り扱うことを予定しているものの漏えい等を防止するために必要かつ適切な措置も含まれる。そのため、以下この条における「個人データ」には、当該個人情報も含まれることに留意する。</u></p> <p>本条における用語の定義は、次のとおりである。</p> <p>(1)～(5) 同左</p> <p>2、3 同左</p>	<p>金融分野ガイドライン第8条第1項 通則ガイドライン3-4-2</p>
<p>(解説)</p> <ul style="list-style-type: none"> 漏えい、滅失及び毀損の定義については、第15条参照 <p>(参照条文：保護法23条、通則ガイドライン3-4-2、金融分野ガイドライン<u>9条</u>)</p>	<p>(解説)</p> <ul style="list-style-type: none"> 漏えい、滅失及び毀損の定義については、第15条参照 <p>(参照条文：保護法23条、通則ガイドライン3-4-2、金融分野ガイドライン<u>8条</u>)</p>	<p>所要の改正</p>
<p>(役職員の監督)</p> <p>第13条 略</p>	<p>(役職員の監督)</p> <p>第13条 略</p>	

【新旧対照表】「個人情報保護指針」

(下線部分改正箇所)

旧	新	根拠法令等
<p>2 協会員は、前項の役職員に対する「必要かつ適切な監督」を以下の体制整備等により行うこととする。</p> <p>(1)、(2) 略</p> <p>(3) 役職員による個人データの持出し等を防ぐため、社内での安全管理措置に定めた事項の遵守状況等の確認及び役職員における個人データの<u>保護に対する</u>点検及び監査制度を整備すること</p>	<p>2 協会員は、前項の役職員に対する「必要かつ適切な監督」を以下の体制整備等により行うこととする。</p> <p>(1)、(2) 同左</p> <p>(3) 役職員による個人データの持出し等を防ぐため、社内での安全管理措置に<u>係る取扱規程</u>に定めた事項の遵守状況等の確認及び役職員における個人データの<u>取扱状況</u>の点検及び監査制度を整備すること</p>	<p>金融分野ガイドライン第9条第3項③</p>
<p>(委託先の監督)</p> <p>第14条 協会員は、個人データの取扱いの全部又は一部を委託（契約の形態や種類を問わず、協会員が他の者に個人データの取扱いの全部又は一部を行わせることを内容とする契約の一切を含む。）する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。</p> <p>なお、当該監督は、個人データが漏えい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ものとする。</p> <p>2 協会員は、個人データを適正に取り扱っていると認められる者を選定し委託するとともに、取扱いを委託した個人データの安全管理措置が図られるよう、個人データの安全管理のための措置を委託先においても確保しなければならない（二段階以上の委託が行われた場合には、委託先の事業者が再委託先等の事業者に対して十分な監督を行っているかについても監督を行うものとする。）。</p> <p>具体的には、以下の対応等が必要である。</p> <p>(1) 個人データの安全管理のため、委託先における組織体制の整備及び安全管理に係る基本方針・取扱規程の策定等の内容を委託先選定の基準に定め、当該基準に従って委託先を選定するとともに、当該基準を定期的に見直すこと。</p> <p>(2) 委託者の監督・監査・報告徴収に関する権限、委託先における個人データの漏えい等の防止及び目的外利用の禁止、再委託に関する条件並びに漏えい等事案が発生した場合の委託先の責任を内容とする安全管理措置を委託契約に盛り込むとともに、定期的又は随時に当該委託契約に定める安全管理措置等の遵守状況を確認し、当該安全管理措置の見直しを行わなければならない。</p>	<p>(委託先の監督)</p> <p>第14条 協会員は、個人データの取扱いの全部又は一部を委託（契約の形態や種類を問わず、協会員が他の者に個人データの取扱いの全部又は一部を行わせることを内容とする契約の一切を含む。）する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。</p> <p>なお、当該監督は、個人データが漏えい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ものとする。</p> <p>2 協会員は、個人データを適正に取り扱っていると認められる者を選定し委託するとともに、取扱いを委託する個人データの安全管理が図られるよう、個人データの安全管理のための措置を委託先においても確保しなければならない（二段階以上の委託が行われた場合には、委託先の事業者が再委託先等の事業者に対して十分な監督を行っているかについても監督を行うものとする。）。</p> <p>具体的には、以下の対応等が必要である。</p> <p>(1) 個人データの安全管理のため、委託先における組織体制の整備及び安全管理に係る基本方針・取扱規程の策定等の内容を委託先選定の基準に定め、当該基準に従って委託先を選定するとともに、当該基準を定期的に見直すこと。</p> <p>(2) 委託者の監督・監査・報告徴収に関する権限、委託先における漏えい等の防止及び目的外利用の禁止、再委託に関する条件並びに漏えい等事案が発生した場合の委託先の責任を内容とする安全管理措置を委託契約に盛り込むとともに、定期的又は随時に当該委託契約に定める安全管理措置等の遵守状況を確認し、当該安全管理措置の見直しを行わなければならない。</p>	<p>金融分野ガイドライン第10条第3項</p> <p>金融分野ガイドライン第10条第3項②</p>
<p>(解説)</p> <p>・委託先には外国の委託先も含まれる。</p> <p>(参照条文：保護法25条、通則ガイドライン3-4-4、金融分野ガイドライン10条)</p>	<p>(解説)</p> <p>・委託先には外国の委託先も含まれる。</p> <p>(参照条文：保護法25条、通則ガイドライン3-4-4、金融分野ガイドライン10条)</p>	

旧	新	根拠法令等
<p>(漏えい等の報告等)</p> <p>第15条 協会員は、その取り扱う個人データの漏えい等その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれ大きいものとして次の各号のいずれかに該当するものが生じたときは、次項以下の定めに従って、当該事態が生じた旨を個人情報保護委員会（保護法第150条の規定により金融庁長官等が報告を受理する権限の委任を受けている場合にあっては金融庁長官等、保護法第170条の規定により地方公共団体の長等が報告を受理する権限に属する事務を行う場合にあっては地方公共団体の長等。第11項において同じ。）に報告しなければならない。ただし、協会員が、他の個人情報取扱事業者から当該個人データの取扱いの全部又は一部の委託を受けた場合であって、当該事態が生じた旨を当該他の個人情報取扱事業者に通知したときは、この限りでない。</p> <p>(1) 要配慮個人情報に含まれる個人データ（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下第1項各号及び次項において同じ。）の漏えい等が発生し、又は発生したおそれがある事態</p> <p>(2) 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態</p> <p>(3) 不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態</p> <p>(4) 個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態</p> <p>2 前項の規定による報告をする場合には、前項各号に定める事態を知った後、速やかに、当該事態に関する次の各号の事項（報告をしようとする時点において把握しているものに限る。第5項において同じ。）を報告しなければならない（この時点での報告を「速報」という。以下同じ。）。</p> <p>(1) 概要</p> <p>(2) 漏えい等が発生し、又は発生したおそれがある個人データの項目</p> <p>(3) 漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数</p> <p>(4) 原因</p> <p>(5) 二次被害又はそのおそれの有無及びその内容</p> <p>(6) 本人への対応の実施状況</p>	<p>(漏えい等の報告等)</p> <p>第15条 協会員は、その取り扱う個人データの漏えい等その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれ大きいものとして次の各号のいずれかに該当するものが生じたときは、次項以下の定めに従って、当該事態が生じた旨を個人情報保護委員会（保護法第150条の規定により金融庁長官等が報告を受理する権限の委任を受けている場合にあっては金融庁長官等、保護法第170条の規定により地方公共団体の長等が報告を受理する権限に属する事務を行う場合にあっては地方公共団体の長等。第11項において同じ。）に報告しなければならない。ただし、協会員が、他の個人情報取扱事業者から当該個人データの取扱いの全部又は一部の委託を受けた場合であって、当該事態が生じた旨を当該他の個人情報取扱事業者に通知したときは、この限りでない。</p> <p>(1) 要配慮個人情報に含まれる個人データ（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下第1項各号及び次項において同じ。）の漏えい等が発生し、又は発生したおそれがある事態</p> <p>(2) 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態</p> <p>(3) 不正の目的をもって行われたおそれがある<u>当該協会員に対する行為による個人データ（当該協会員が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているものを含む。）</u>の漏えい等が発生し、又は発生したおそれがある事態</p> <p>(4) 個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態</p> <p>2 前項の規定による報告をする場合には、前項各号に定める事態を知った後、速やかに、当該事態に関する次の各号の事項（報告をしようとする時点において把握しているものに限る。第5項において同じ。）を報告しなければならない（この時点での報告を「速報」という。以下同じ。）。</p> <p>(1) 概要</p> <p>(2) 漏えい等が発生し、又は発生したおそれがある個人データ<u>（前項第(3)号に定める事態については、同号に規定する個人情報を含む。次号において同じ。）</u>の項目</p> <p>(3) 漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数</p> <p>(4) 原因</p> <p>(5) 二次被害又はそのおそれの有無及びその内容</p> <p>(6) 本人への対応の実施状況</p>	<p>保護法施行規則第7条第1項第3号 通則ガイドライン3-5-3-1(3)</p> <p>保護法施行規則第8条第1項第2号</p>

【新旧対照表】 「個人情報保護指針」

(下線部分改正箇所)

旧	新	根拠法令等
<p>(7) 公表の実施状況 (8) 再発防止のための措置 (9) その他参考となる事項 3～11 略</p>	<p>(7) 公表の実施状況 (8) 再発防止のための措置 (9) その他参考となる事項 3～11 同左</p>	
<p>(解説) (新設)</p> <p><u>(1) 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をいう。</u> なお、個人データを第三者に閲覧されないうちに全てを回収した場合は、漏えいに該当しない。また、協会員が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は、漏えいに該当しない。</p> <p>【個人データの漏えいに該当する事例】 事例1) 個人データが記載された書類を第三者に誤送付した場合 事例2) 個人データを含むメールを第三者に誤送信した場合 事例3) システムの設定ミス等によりインターネット上で個人データの閲覧が可能な状態となっていた場合 事例4) 個人データが記載又は記録された書類・媒体等が盗難された場合 事例5) 不正アクセス等により第三者に個人データを含む情報が窃取された場合</p> <p>(新設)</p> <p><u>(2) 個人データの「滅失」とは、個人データの内容が失われることをいう。</u></p>	<p>(解説)</p> <p><u>(1) 第1項に規定する「個人データ」とは、協会員が取り扱う個人データをいう。</u> <u>ただし、同項第(3)号に規定する「個人データ」には、「当該協会員が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているもの」が含まれる。</u> <u>そのため、同号に定める事態との関係では、解説(2)から(4)までにおける「個人データ」は、協会員が取り扱う個人データに加え、「当該協会員が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているもの」を含む。</u> <u>同号に定める事態について、詳細は解説(6)を参照のこと。</u></p> <p><u>(2) 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をいう。</u> なお、個人データを第三者に閲覧されないうちに全てを回収した場合は、漏えいに該当しない。また、協会員が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は、漏えいに該当しない。</p> <p>【個人データの漏えいに該当する事例】 事例1) 個人データが記載された書類を第三者に誤送付した場合 事例2) 個人データを含むメールを第三者に誤送信した場合 事例3) システムの設定ミス等によりインターネット上で個人データの閲覧が可能な状態となっていた場合 事例4) 個人データが記載又は記録された書類・媒体等が盗難された場合 事例5) 不正アクセス等により第三者に個人データを含む情報が窃取された場合</p> <p><u>事例6) 協会員のウェブサイトの入力ページが第三者に改ざんされ、ユーザーが当該ページに入力した個人情報が、当該第三者に送信された場合であり、かつ、当該協会員が、当該ページに入力される個人情報を個人情報データベース等へ入力することを予定していたとき</u></p> <p><u>(3) 個人データの「滅失」とは、個人データの内容が失われることをいう。</u></p>	<p>通則ガイドライン3-5-1-1</p> <p>通則ガイドライン3-5-1-2 事例6)</p>

旧	新	根拠法令等
<p>なお、下記の場合であっても、その内容と同じデータが他に保管されている場合は、滅失に該当しない。また、協会員が合理的な理由により個人データを削除する場合は、滅失に該当しない。</p> <p>【個人データの滅失に該当する事例】</p> <p>事例1) 個人情報データベース等から出力された氏名等が記載された帳票等を誤って廃棄した場合 (注) 当該帳票等が適切に廃棄されていない場合には、個人データの漏えいに該当する場合がある。</p> <p>事例2) 個人データが記載又は記録された書類・媒体等を社内で紛失した場合 (注) 社外に流出した場合には、個人データの漏えいに該当する。</p> <p><u>③</u> 略</p> <p><u>④</u> 報告すべき事態が発覚した場合に講じるべき措置 (第10項) 協会員が本条に基づき報告すべき事態 (第1項、第6項及び第7項に規定する事態) が発覚した場合に当該事態の内容等に応じて講じるべき必要な措置の内容は、次のとおりである。</p> <p>① 事業者内部における報告及び被害の拡大防止 責任ある立場の者に直ちに報告するとともに、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を講ずる。</p> <p>② 事実関係の調査及び原因の究明 漏えい等事案の事実関係の調査及び原因の究明に必要な措置を講ずる。</p> <p>③ 影響範囲の特定 上記②で把握した事実関係による影響範囲の特定のために必要な措置を講ずる。</p> <p>④ 再発防止策の検討及び実施 上記②の結果を踏まえ、漏えい等事案の再発防止策の検討及び実施に必要な措置を講ずる。</p> <p>⑤ 個人情報保護委員会への報告及び本人への通知 <u>解説(5)から(15)</u>を参照のこと。 なお、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、速やかに公表することが望ましい。</p> <p><u>⑤</u> 保護法に基づく報告対象事態 (第1項) 協会員は、次の①から④までに掲げる事態 (以下「保護法報告対象事態」という。) を知ったときは、個人情報保護委員会から権限の委任を受けている監督当局 (財務局長若しくは財務支局長又は都道府県知事) 及び本協会に報告しなければならない (第1項、第11項)。</p>	<p>なお、下記の場合であっても、その内容と同じデータが他に保管されている場合は、滅失に該当しない。また、協会員が合理的な理由により個人データを削除する場合は、滅失に該当しない。</p> <p>【個人データの滅失に該当する事例】</p> <p>事例1) 個人情報データベース等から出力された氏名等が記載された帳票等を誤って廃棄した場合 (注) 当該帳票等が適切に廃棄されていない場合には、個人データの漏えいに該当する場合がある。</p> <p>事例2) 個人データが記載又は記録された書類・媒体等を社内で紛失した場合 (注) 社外に流出した場合には、個人データの漏えいに該当する。</p> <p><u>④</u> 同左</p> <p><u>⑤</u> 報告すべき事態が発覚した場合に講じるべき措置 (第10項) 協会員が本条に基づき報告すべき事態 (第1項、第6項及び第7項に規定する事態) が発覚した場合に当該事態の内容等に応じて講じるべき必要な措置の内容は、次のとおりである。</p> <p>① 事業者内部における報告及び被害の拡大防止 責任ある立場の者に直ちに報告するとともに、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を講ずる。</p> <p>② 事実関係の調査及び原因の究明 漏えい等事案の事実関係の調査及び原因の究明に必要な措置を講ずる。</p> <p>③ 影響範囲の特定 上記②で把握した事実関係による影響範囲の特定のために必要な措置を講ずる。</p> <p>④ 再発防止策の検討及び実施 上記②の結果を踏まえ、漏えい等事案の再発防止策の検討及び実施に必要な措置を講ずる。</p> <p>⑤ 個人情報保護委員会への報告及び本人への通知 <u>解説(6)から(16)</u>を参照のこと。 なお、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、速やかに公表することが望ましい。</p> <p><u>⑥</u> 保護法に基づく報告対象事態 (第1項) 協会員は、次の①から④までに掲げる事態 (以下「保護法報告対象事態」という。) を知ったときは、個人情報保護委員会から権限の委任を受けている監督当局 (財務局長若しくは財務支局長又は都道府県知事) 及び本協会に報告しなければならない (第1項、第11項)。</p>	

旧	新	根拠法令等
<p>なお、保護法報告対象事態に該当しない漏えい等事案であっても、協会員は個人情報保護委員会及び本協会に任意の報告をすることができる。</p> <p>保護法報告対象事態における「おそれ」については、その時点で判明している事実関係に基づいて個別の事案ごとに蓋然性を考慮して判断することになる。漏えい等が発生したおそれについては、その時点で判明している事実関係からして、漏えい等が疑われるものの漏えい等が生じた確証がない場合がこれに該当する。</p> <p>① 要配慮個人情報に含まれる個人データの漏えい等が発生し、又は発生したおそれがある事態（第1項第(1)号関係）</p> <p>【報告を要する事例】</p> <p>事例1) 従業員の健康診断等の結果を含む個人データが漏えいした場合</p> <p>② 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態（第1項第(2)号関係）</p> <p>財産的被害が生じるおそれについては、対象となった個人データの性質・内容等を踏まえ、財産的被害が発生する蓋然性を考慮して判断する。</p> <p>【報告を要する事例】</p> <p>事例1) ECサイトからクレジットカード番号を含む個人データが漏えいした場合</p> <p>事例2) 送金や決済機能のあるウェブサービスのログインIDとパスワードの組み合わせを含む個人データが漏えいした場合</p> <p>③ 不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態（第1項第(3)号関係）</p> <p>「不正の目的をもって」<u>漏えい等が発生させた</u>主体には、第三者のみならず、従業者も含まれる。</p>	<p>なお、保護法報告対象事態に該当しない漏えい等事案であっても、協会員は個人情報保護委員会及び本協会に任意の報告をすることができる。</p> <p>保護法報告対象事態における「おそれ」については、その時点で判明している事実関係に基づいて個別の事案ごとに蓋然性を考慮して判断することになる。漏えい等が発生したおそれについては、その時点で判明している事実関係からして、漏えい等が疑われるものの漏えい等が生じた確証がない場合がこれに該当する。</p> <p>① 要配慮個人情報に含まれる個人データの漏えい等が発生し、又は発生したおそれがある事態（第1項第(1)号関係）</p> <p>【報告を要する事例】</p> <p>事例1) 従業員の健康診断等の結果を含む個人データが漏えいした場合</p> <p>② 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態（第1項第(2)号関係）</p> <p>財産的被害が生じるおそれについては、対象となった個人データの性質・内容等を踏まえ、財産的被害が発生する蓋然性を考慮して判断する。</p> <p>【報告を要する事例】</p> <p>事例1) ECサイトからクレジットカード番号を含む個人データが漏えいした場合</p> <p>事例2) 送金や決済機能のあるウェブサービスのログインIDとパスワードの組み合わせを含む個人データが漏えいした場合</p> <p>③ 不正の目的をもって行われたおそれがある<u>当該協会員に対する行為による個人データ（当該協会員が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているものを含む。）</u>の漏えい等が発生し、又は発生したおそれがある事態（第1項第(3)号関係）</p> <p>「不正の目的をもって行われたおそれがある<u>当該協会員に対する行為</u>」（以下「不正行為」という。）の主体には、第三者のみならず、従業者も含まれる。<u>また、不正行為の相手方である「当該協会員」には、当該協会員が第三者に個人データの取扱いを委託している場合における当該第三者（委託先）及び当該協会員が個人データを取り扱うに当たって第三者の提供するサービスを利用している場合における当該第三者も含まれる。</u></p> <p><u>当該協会員が「取得しようとしている個人情報」に該当するかどうかは、当該協会員が用いている個人情報の取得手段等を考慮して客観的に判断する。</u></p> <p><u>個人情報データベース等へ入力すること等を予定してい</u></p>	<p>根拠法令等</p> <p>通則ガイドライン3-5-3-1(3)</p>

旧	新	根拠法令等
<p>(新設)</p> <p>【報告を要する事例】 事例1) 不正アクセスにより個人データが漏えいした場合</p> <p>(注) サイバー攻撃の事案について、「漏えい」が発生したおそれがある事態に該当し得る事例としては、例えば、次のイからニが考えられる。</p> <p>イ 個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において外部からの不正アクセスによりデータが窃取された痕跡が認められた場合</p> <p>ロ 個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において、情報を窃取する振る舞いが判明しているマルウェアの感染が確認された場合</p> <p>ハ マルウェアに感染したコンピュータに不正な指令を送り、制御するサーバ (C&Cサーバ) が使用しているものとして知られているIPアドレス・FQDN (Fully Qualified Domain Nameの略。サブドメイン名及びドメイン名からなる文字列であり、ネットワーク上のコンピュータ (サーバ等) を特定するもの。) への通信が確認された場合</p> <p>ニ 不正検知を行う公的機関、セキュリティ・サービス・プロバイダ、専門家等の第三者から、漏えいのおそれについて、一定の根拠に基づく連絡を受けた場合</p> <p>事例2) ランサムウェア等により個人データが暗号化され、復元できなくなった場合</p> <p>事例3) 個人データが記載又は記録された書類・媒体等が盗</p>	<p><u>ば、最終的に個人情報に該当しない統計情報への加工を行うことを予定している場合等であっても、「個人データとして取り扱われることが予定されている」に該当する。</u></p> <p><u>(注) 協会員が、個人データとして取り扱うことを予定している個人情報の取扱いを第三者に委託する場合であって、当該第三者 (委託先) が当該個人情報を個人データとして取り扱う予定はないときも、ここにいう「協会員が第三者に個人データの取扱いを委託している場合」に該当する。</u></p> <p>【報告を要する事例】 事例1) 不正アクセスにより個人データ <u>(個人情報データベース等へ入力する予定の個人情報を含む。以下、事例5) まで同じ。)</u> が漏えいした場合</p> <p>事例2) ランサムウェア等により個人データが暗号化され、復元できなくなった場合</p> <p>事例3) 個人データが記載又は記録された書類・媒体等が盗</p>	<p>通則ガイドライン2-5-3-1(※3)</p> <p>通則ガイドライン3-5-3-1(3) 【報告を要する事例】</p> <p>事例8) の下へ移設</p>

旧	新	根拠法令等
<p>難された場合 事例4) 従業者が顧客の個人データを不正に持ち出して第三者に提供した場合</p> <p>(注) 従業者による個人データの持ち出しの事案について、「漏えい」が発生したおそれがある事態に該当し得る事例としては、例えば、個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において、通常の業務で必要としないアクセスによりデータが窃取された痕跡が認められた場合が考えられる。</p>	<p>難された場合 事例4) 従業者が顧客の個人データを不正に持ち出して第三者に提供した場合</p> <p>(注) 従業者による個人データ <u>又は個人情報</u>の持ち出しの事案について、「漏えい」が発生したおそれがある事態に該当し得る事例としては、例えば、個人データ <u>又は個人情報</u>を格納しているサーバや、当該サーバにアクセス権限を有する端末において、通常の業務で必要としないアクセスによりデータが窃取された痕跡が認められた場合が考えられる。</p>	<p>通則ガイドライン3-5-3-1(※5)</p>
<p>(新設)</p>	<p><u>事例5) 従業者の私用の端末又は取引先の端末が情報を窃取するマルウェアに感染し、その後、当該端末と協会のサーバとの電気通信に起因して、当該サーバも当該マルウェアに感染し、個人データが漏えいした場合</u></p>	<p>通則ガイドライン3-5-3-1(3) 【報告を要する事例】</p>
<p>(新設)</p>	<p><u>事例6) 協会のウェブサイトの入力ページが第三者に改ざんされ、ユーザーが当該ページに入力した個人情報が当該第三者に送信された場合であり、かつ、当該協会が、当該ページに入力される個人情報を個人情報データベース等へ入力することを予定していたとき</u></p>	
<p>(新設)</p>	<p><u>事例7) 協会のウェブサイト上に設置された、入力ページに遷移するためのリンクやボタンが第三者に改ざんされ、当該リンクやボタンをユーザーがクリックした結果、偽の入力ページに遷移し、当該ユーザーが当該偽の入力ページに入力した個人情報が当該第三者に送信された場合であり、かつ、当該協会が、当該協会の入力ページに入力される個人情報を個人情報データベース等へ入力することを予定していたとき</u></p>	
<p>(新設)</p>	<p><u>事例8) 協会が、第三者により宛先の改ざんされた返信用封筒を顧客に送付した結果、当該返信用封筒により返信されたアンケート用紙に記入された個人情報が当該第三者に送付された場合であり、かつ、当該協会が、当該個人情報を個人情報データベース等へ入力することを予定していたとき</u></p> <p>(注) サイバー攻撃の事案について、「漏えい」が発生したおそれがある事態に該当し得る事例としては、例えば、次のイからホが考えられる。 イ 個人データ <u>(個人情報データベース等へ入力する予定の個人情報を含む。ロにおいて同じ。)</u>を格納して</p>	<p>通則ガイドライン3-5-3-1(※4) 事例1) の下より移設</p>

旧	新	根拠法令等
<p>(新設)</p> <p>④ 個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態（第1項第(4)号関係） 「個人データに係る本人の数」は、当該協会員が取り扱う個人データのうち、漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数をいう。「個人データに係る本人の数」について、事態が発覚した当初1,000人以下であっても、その後1,000人を超えた場合には、1,000人を超えた時点で第1項第(4)号に該当することになる。本人の数が確定できない漏えい等において、漏えい等が発生したおそれがある個人データに係る本人の数が最大1,000人を超える場合には、第1項第(4)号に該当する。 事例) システムの設定ミス等によりインターネット上で個人データの閲覧が可能な状態となり、当該個人データに係る本人の数が1,000人を超える場合 なお、漏えい等が発生し、又は発生したおそれがある個人データについて、高度な暗号化等の秘匿化がされている場合等、「高度な暗号化その他の個人の権利利益を保護するために必要な措</p>	<p>いるサーバや、当該サーバにアクセス権限を有する端末において外部からの不正アクセスによりデータが窃取された痕跡が認められた場合 ロ 個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において、情報を窃取する振る舞いが判明しているマルウェアの感染が確認された場合 ハ マルウェアに感染したコンピュータに不正な指令を送り、制御するサーバ（C&Cサーバ）が使用しているものとして知られているIPアドレス・FQDN（Fully Qualified Domain Nameの略。サブドメイン名及びドメイン名からなる文字列であり、ネットワーク上のコンピュータ（サーバ等）を特定するもの。）への通信が確認された場合 <u>ニ 個人情報の取得手段であるウェブページを構成するファイルを保存しているサーバや、当該サーバにアクセス権限を有する端末において、外部からの不正アクセスにより、当該ファイルに、当該ウェブページに入力された情報を窃取するような改ざんがされた痕跡が確認された場合</u> ホ 不正検知を行う公的機関、セキュリティ・サービス・プロバイダ、専門家等の第三者から、漏えいのおそれについて、一定の根拠に基づく連絡を受けた場合</p> <p>④ 個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態（第1項第(4)号関係） 「個人データに係る本人の数」は、当該協会員が取り扱う個人データのうち、漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数をいう。「個人データに係る本人の数」について、事態が発覚した当初1,000人以下であっても、その後1,000人を超えた場合には、1,000人を超えた時点で第1項第(4)号に該当することになる。本人の数が確定できない漏えい等において、漏えい等が発生したおそれがある個人データに係る本人の数が最大1,000人を超える場合には、第1項第(4)号に該当する。 事例) システムの設定ミス等によりインターネット上で個人データの閲覧が可能な状態となり、当該個人データに係る本人の数が1,000人を超える場合 なお、漏えい等が発生し、又は発生したおそれがある個人データ <u>又は個人情報</u> について、高度な暗号化等の秘匿化がされている場合等、「高度な暗号化その他の個人の権利利益を保護するため</p>	<p>根拠法令等</p> <p>通則ガイドライン3-5-3-1</p>

旧	新	根拠法令等
<p>置」が講じられている場合については、報告を要しない。</p> <p>(6) 報告義務の主体 漏えい等報告の義務を負う主体は、漏えい等が発生し、又は発生したおそれがある個人データを取り扱う協会員である。</p> <p>個人データの取扱いを委託している場合においては、委託元と委託先の双方が個人データを取り扱っていることになるため、保護法報告対象事態に該当する場合には、原則として委託元と委託先の双方が報告する義務を負う。この場合、委託元及び委託先の連名で報告することができる。なお、委託先が、報告義務を負っている委託元に当該事態が発生したことを通知したときは、委託先は報告義務を免除される（第1項ただし書参照）。</p> <p>また、委託元から委託先にある個人データ（個人データA）の取扱いを委託している場合であって、別の個人データ（個人データB）の取扱いを委託していないときには、個人データBについて、委託元において報告対象事態が発生した場合であっても、委託先は報告義務を負わず、委託元のみが報告義務を負うことになる。</p> <p>(7) 「速報」について（第2項） 協会員は、保護法報告対象事態を知ったときは、速やかに、個人情報保護委員会及び本協会に報告しなければならない。 報告期限の起算点となる「知った」時点については、個別の事案ごとに判断されるが、協会員が法人である場合には、いずれかの部署が当該事態を知った時点を基準とする。「速やか」の日数の目安については、個別の事案によるものの、協会員が当該事態を知った時点から概ね3～5日以内である。 個人情報保護委員会への漏えい等報告については、次の①から⑨までに掲げる事項を、原則として、個人情報保護委員会のホームページの報告フォームに入力する方法により行う。速報時点での報告内容については、報告をしようとする時点において把握している内容を報告すれば足りる。</p> <p>① 「概要」 当該事態の概要について、発生日、発覚日、発生事案、発見者、第15条第1項各号該当性、委託元及び委託先の有無、事実経過等を報告する。</p> <p>② 「漏えい等が発生し、又は発生したおそれがある個人データ</p>	<p>に必要な措置」が講じられている場合については、報告を要しない。</p> <p>(7) 報告義務の主体 漏えい等報告の義務を負う主体は、<u>原則として、漏えい等が発生し、又は発生したおそれがある個人データを取り扱う協会員である。ただし、第1項第(3)号に定める事態について漏えい等報告の義務を負う主体は、漏えい等が発生し、又は発生したおそれがある個人データ又は個人情報を取り扱い、又は取得しようとしている協会員である（解説(1)参照）。</u></p> <p>個人データの取扱いを委託している場合においては、委託元と委託先の双方が個人データ<u>又は個人情報</u>を取り扱っており、<u>又は取得しようとして</u>いることになるため、保護法報告対象事態に該当する場合には、原則として委託元と委託先の双方が報告する義務を負う。この場合、委託元及び委託先の連名で報告することができる。なお、委託先が、報告義務を負っている委託元に当該事態が発生したことを通知したときは、委託先は報告義務を免除される（第1項ただし書参照）。</p> <p>また、委託元から委託先にある個人データ（個人データA）の取扱いを委託している場合であって、別の個人データ（個人データB）の取扱いを委託していないときには、個人データBについて、委託元において報告対象事態が発生した場合であっても、委託先は報告義務を負わず、委託元のみが報告義務を負うことになる。</p> <p>(8) 「速報」について（第2項） 協会員は、保護法報告対象事態を知ったときは、速やかに、個人情報保護委員会及び本協会に報告しなければならない。 報告期限の起算点となる「知った」時点については、個別の事案ごとに判断されるが、協会員が法人である場合には、いずれかの部署が当該事態を知った時点を基準とする。「速やか」の日数の目安については、個別の事案によるものの、協会員が当該事態を知った時点から概ね3～5日以内である。 個人情報保護委員会への漏えい等報告については、次の①から⑨までに掲げる事項を、原則として、個人情報保護委員会のホームページの報告フォームに入力する方法により行う。速報時点での報告内容については、報告をしようとする時点において把握している内容を報告すれば足りる。</p> <p>① 「概要」 当該事態の概要について、発生日、発覚日、発生事案、発見者、第15条第1項各号該当性、委託元及び委託先の有無、事実経過等を報告する。</p> <p>② 「漏えい等が発生し、又は発生したおそれがある個人データ</p>	<p>根拠法令等</p> <p>通則ガイドライン3-5-3-2</p>

旧	新	根拠法令等
<p>の項目」</p> <p>漏えい等が発生し、又は発生したおそれがある個人データの項目について、媒体や種類（顧客情報、従業員情報の別等）とともに報告する。</p> <p>③ 「漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数」 漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数について報告する。</p> <p>④ 「原因」 当該事態が発生した原因について、当該事態が発生した主体（報告者又は委託先）とともに報告する。</p> <p>⑤ 「二次被害又はそのおそれの有無及びその内容」 当該事態に起因して発生する被害又はそのおそれの有無及びその内容について報告する。</p> <p>⑥ 「本人への対応の実施状況」 当該事態を知った後、本人に対して行った措置（通知を含む。）の実施状況について報告する。</p> <p>⑦ 「公表の実施状況」 当該事態に関する公表の実施状況について報告する。</p> <p>⑧ 「再発防止のための措置」 漏えい等事案が再発することを防止するために講ずる措置について、実施済みの措置と今後実施予定の措置に分けて報告する。</p> <p>⑨ 「その他参考となる事項」 上記の①から⑧までの事項を補完するため、個人情報保護委員会が当該事態を把握する上で参考となる事項を報告する。</p> <p><u>⑧</u> 「確報」について（第3項） 協会員は、保護法報告対象事態を知ったときは、速報に加え、30日以内（第1項第3号の事態においては60日以内。同号の事態に加え、同条第(1)号、第(2)号又は第(4)号の事態にも該当する場合も60日以内。）に個人情報保護委員会及び本協会に報告しなければならない。30日以内又は60日以内は報告期限であり、可能である場合には、より早期に報告することが望ましい。 報告期限の起算点となる「知った」時点については、速報と同様に、協会員が法人である場合には、いずれかの部署が当該事態を知った時点を基準とし、確報の報告期限の算定に当たっては、その時点を1日目とする。 確報においては、<u>解説(7)</u>①～⑨までに掲げる事項の全てを報告</p>	<p><u>（前項第(3)号に定める事態については、同号に規定する個人情報を含む。次号において同じ。）</u>の項目」</p> <p>漏えい等が発生し、又は発生したおそれがある個人データ<u>（第1項第(3)号に定める事態については、同号に規定する個人情報を含む。）</u>の項目について、媒体や種類（顧客情報、従業員情報の別等）とともに報告する。</p> <p>③ 「漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数」 漏えい等が発生し、又は発生したおそれがある個人データ<u>（第1項第(3)号に定める事態については、同号に規定する個人情報を含む。）</u>に係る本人の数について報告する。</p> <p>④ 「原因」 当該事態が発生した原因について、当該事態が発生した主体（報告者又は委託先）とともに報告する。</p> <p>⑤ 「二次被害又はそのおそれの有無及びその内容」 当該事態に起因して発生する被害又はそのおそれの有無及びその内容について報告する。</p> <p>⑥ 「本人への対応の実施状況」 当該事態を知った後、本人に対して行った措置（通知を含む。）の実施状況について報告する。</p> <p>⑦ 「公表の実施状況」 当該事態に関する公表の実施状況について報告する。</p> <p>⑧ 「再発防止のための措置」 漏えい等事案が再発することを防止するために講ずる措置について、実施済みの措置と今後実施予定の措置に分けて報告する。</p> <p>⑨ 「その他参考となる事項」 上記の①から⑧までの事項を補完するため、個人情報保護委員会が当該事態を把握する上で参考となる事項を報告する。</p> <p><u>⑨</u> 「確報」について（第3項） 協会員は、保護法報告対象事態を知ったときは、速報に加え、30日以内（第1項第(3)号の事態においては60日以内。同号の事態に加え、同条第(1)号、第(2)号又は第(4)号の事態にも該当する場合も60日以内。）に個人情報保護委員会及び本協会に報告しなければならない。30日以内又は60日以内は報告期限であり、可能である場合には、より早期に報告することが望ましい。 報告期限の起算点となる「知った」時点については、速報と同様に、協会員が法人である場合には、いずれかの部署が当該事態を知った時点を基準とし、確報の報告期限の算定に当たっては、その時点を1日目とする。 確報においては、<u>解説(8)</u>①～⑨までに掲げる事項の全てを報告</p>	<p>通則ガイドライン3-5-3-3(2)</p> <p>通則ガイドライン3-5-3-3(3)</p>

旧	新	根拠法令等
<p>しなければならない。確報を行う時点（保護法報告対象事態を知った日から30日以内又は60日以内）において、合理的努力を尽くした上で、一部の事項が判明しておらず、全ての事項を報告することができない場合には、その時点で把握している内容を報告し、判明次第、報告を追完するものとする。</p> <p>(注1) 速報の時点で全ての事項を報告できる場合には、1回の報告で速報と確報を兼ねることができる。</p> <p>(注2) 確報の報告期限（30日以内又は60日以内）の算定に当たっては、土日・祝日も含める。ただし、30日目又は60日目が土日、祝日又は年末年始閉庁日（12月29日～1月3日）の場合は、その翌日を報告期限とする（行政機関の休日に関する法律（昭和63年法律第91号）第2条）。</p> <p><u>9</u> 委託元への通知による例外 委託先は、個人情報保護委員会への報告義務を負っている委託元に対し、<u>解説(7)</u>①～⑨までに掲げる事項のうち、その時点で把握しているものを通知したときは、報告義務を免除される（第1項ただし書参照）。委託元への通知については、速報としての報告と同様に、保護法報告対象事態を知った後、速やかに行わなければならない。「速やか」の日数の目安については、個別の事案によるものの、委託先が当該事態の発生を知った時点から概ね3～5日以内である。 この場合、委託先から通知を受けた委託元が報告をすることになる。委託元は、通常、遅くとも委託先から通知を受けた時点で、保護法報告対象事態を知ったこととなり、速やかに報告を行わなければならない。 なお、通知を行った委託先は、委託元から報告するに当たり、事態の把握を行うとともに、必要に応じて委託元の漏えい等報告に協力することが求められる。</p> <p><u>10</u> 略</p> <p><u>11</u> 本人への通知、通知対象となる事態及び通知義務の主体 協会員は、保護法報告対象事態を知ったときは、本人への通知を行わなければならない（第8項）。 通知義務を負う主体は、漏えい等が発生し、又は発生したおそれがある個人データを取り扱う協会員である。</p>	<p>しなければならない。確報を行う時点（保護法報告対象事態を知った日から30日以内又は60日以内）において、合理的努力を尽くした上で、一部の事項が判明しておらず、全ての事項を報告することができない場合には、その時点で把握している内容を報告し、判明次第、報告を追完するものとする。</p> <p>(注1) 速報の時点で全ての事項を報告できる場合には、1回の報告で速報と確報を兼ねることができる。</p> <p>(注2) 確報の報告期限（30日以内又は60日以内）の算定に当たっては、土日・祝日も含める。ただし、30日目又は60日目が土日、祝日又は年末年始閉庁日（12月29日～1月3日）の場合は、その翌日を報告期限とする（行政機関の休日に関する法律（昭和63年法律第91号）第2条）。</p> <p><u>10</u> 委託元への通知による例外 委託先は、個人情報保護委員会への報告義務を負っている委託元に対し、<u>解説(8)</u>①～⑨までに掲げる事項のうち、その時点で把握しているものを通知したときは、報告義務を免除される（第1項ただし書参照）。委託元への通知については、速報としての報告と同様に、保護法報告対象事態を知った後、速やかに行わなければならない。「速やか」の日数の目安については、個別の事案によるものの、委託先が当該事態の発生を知った時点から概ね3～5日以内である。 この場合、委託先から通知を受けた委託元が報告をすることになる。委託元は、通常、遅くとも委託先から通知を受けた時点で、保護法報告対象事態を知ったこととなり、速やかに報告を行わなければならない。 なお、通知を行った委託先は、委託元から報告するに当たり、事態の把握を行うとともに、必要に応じて委託元の漏えい等報告に協力することが求められる。</p> <p><u>11</u> 同左</p> <p><u>12</u> 本人への通知、通知対象となる事態及び通知義務の主体 協会員は、保護法報告対象事態を知ったときは、本人への通知を行わなければならない（第8項）。 通知義務を負う主体は、<u>原則として、漏えい等が発生し、又は発生したおそれがある個人データを取り扱う協会員である。ただし、第1項第(3)号に定める事態について本人への通知の義務を負う主体は、漏えい等が発生し、又は発生したおそれがある個人データ又は個人情報を取り扱い、又は取得しようとしている協会員である。（解説(1)参照）。</u></p>	<p>根拠法令等</p> <p>通則ガイドライン3-5-4-1</p>

旧	新	根拠法令等
<p>個人データの取扱いを委託している場合において、委託先が、報告義務を負っている委託元に<u>解説(7)①～⑨</u>までに掲げる事項のうち、その時点で把握しているものを通知したときは、委託先は報告義務を免除されるとともに、本人への通知義務も免除される。</p> <p>また、協会員は、第9項各号のいずれかの事態を知ったときも、上記に準じて本人への通知等を行う努力義務を負う（第9項）。</p> <p>金融機関が取り扱う情報の性質等に鑑み、基本的には全ての漏えい等事案について本人への通知等を行うことが望ましいとされる。なお、例えば、漏えい等した個人データについて、高度な暗号化等の秘匿化措置が講じられている場合や、漏えいした個人データを即時に回収した場合等、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場合等には、本人への通知を要しない。</p> <p><u>12</u> 通知の時間的制限</p> <p>協会員は、保護法報告対象事態を知ったときは、当該事態の状況に応じて速やかに、本人への通知を行わなければならない。</p> <p>「当該事態の状況に応じて速やかに」とは、速やかに通知を行うことを求めるものであるが、具体的に通知を行う時点は、個別の事案において、その時点で把握している事態の内容、通知を行うことで本人の権利利益が保護される蓋然性、本人への通知を行うことで生じる弊害等を勘案して判断する。</p> <p>【その時点で通知を行う必要があるとはいえないと考えられる事例】</p> <p>事例1) インターネット上の掲示板等に漏えいした複数の個人データがアップロードされており、<u>個人情報取扱事業者</u>において当該掲示板等の管理者に削除を求める等、必要な初期対応が完了しておらず、本人に通知することで、かえって被害が拡大するおそれがある場合</p> <p>事例2) 漏えい等のおそれが生じたものの、事案がほとんど判明しておらず、その時点で本人に通知したとしても、本人がその権利利益を保護するための措置を講じられる見込みがなく、かえって混乱が生じるおそれがある場合</p> <p><u>13</u> 通知の内容</p>	<p>個人データの取扱いを委託している場合においては、<u>委託元と委託先の双方が個人データ又は個人情報を取り扱い、又は取得しようとしていること</u>になるため、<u>報告対象事態に該当する場合には、原則として委託元と委託先の双方が本人への通知を行う義務を負う</u>。委託先が、報告義務を負っている委託元に<u>解説(8)①～⑨</u>までに掲げる事項のうち、その時点で把握しているものを通知したときは、委託先は報告義務を免除されるとともに、本人への通知義務も免除される。<u>なお、委託元への通知を行った委託先は、必要に応じて委託元による本人への通知に協力することが求められる。</u></p> <p>また、協会員は、第9項各号のいずれかの事態を知ったときも、上記に準じて本人への通知等を行う努力義務を負う（第9項）。</p> <p>金融機関が取り扱う情報の性質等に鑑み、基本的には全ての漏えい等事案について本人への通知等を行うことが望ましいとされる。なお、例えば、漏えい等した個人データについて、高度な暗号化等の秘匿化措置が講じられている場合や、漏えいした個人データを即時に回収した場合等、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場合等には、本人への通知を要しない。</p> <p><u>13</u> 通知の時間的制限</p> <p>協会員は、保護法報告対象事態を知ったときは、当該事態の状況に応じて速やかに、本人への通知を行わなければならない。</p> <p>「当該事態の状況に応じて速やかに」とは、速やかに通知を行うことを求めるものであるが、具体的に通知を行う時点は、個別の事案において、その時点で把握している事態の内容、通知を行うことで本人の権利利益が保護される蓋然性、本人への通知を行うことで生じる弊害等を勘案して判断する。</p> <p>【その時点で通知を行う必要があるとはいえないと考えられる事例】</p> <p>事例1) インターネット上の掲示板等に漏えいした複数の個人データがアップロードされており、<u>協会員</u>において当該掲示板等の管理者に削除を求める等、必要な初期対応が完了しておらず、本人に通知することで、かえって被害が拡大するおそれがある場合</p> <p>事例2) 漏えい等のおそれが生じたものの、事案がほとんど判明しておらず、その時点で本人に通知したとしても、本人がその権利利益を保護するための措置を講じられる見込みがなく、かえって混乱が生じるおそれがある場合</p> <p><u>14</u> 通知の内容</p>	

旧	新	根拠法令等
<p>本人へ通知すべき事項については、漏えい等報告における報告事項のうち、「概要」、「漏えい等が発生し、又は発生したおそれがある個人データの項目」、「原因」、「二次被害又はそのおそれの有無及びその内容」及び「その他参考となる事項」(解説(7)参照)に限られている。これらの事項が全て判明するまで本人への通知をする必要がないというのではなく、本人への通知は、「当該事態の状況に応じて速やかに」行う必要がある。</p> <p>本人への通知については、「本人の権利利益を保護するために必要な範囲において」行うものである。</p> <p>また、当初保護法報告対象事態に該当すると判断したものの、その後実際には保護法報告対象事態に該当していなかったことが判明した場合には、本人への通知が「本人の権利利益を保護するために必要な範囲において」行うものであることに鑑み、本人への通知は不要である。</p> <p>(注) 第2項第(9)号に定める「その他参考となる事項」については、本人への通知を補完するため、本人にとって参考となる事項をいい、例えば、本人が自らの権利利益を保護するために取り得る措置が考えられる。</p> <p>【本人の権利利益を保護するために必要な範囲において通知を行う事例】</p> <p>事例1) 不正アクセスにより個人データが漏えいした場合において、その原因を本人に通知するに当たり、個人情報保護委員会に報告した詳細な内容ではなく、必要な内容を選択して本人に通知すること。</p> <p>事例2) 漏えい等が発生した個人データの項目が本人ごとに異なる場合において、当該本人に関係する内容のみを本人に通知すること。</p> <p>(14)、(15) 略</p> <p>(参照条文：保護法26条、施行規則7条から10条、通則ガイドライン3-5、金融分野ガイドライン11条)</p>	<p>本人へ通知すべき事項については、漏えい等報告における報告事項のうち、「概要」、「漏えい等が発生し、又は発生したおそれがある個人データ <u>(前項第(3)号に定める事態については、同号に規定する個人情報を含む。次号において同じ。)</u>」の項目、「原因」、「二次被害又はそのおそれの有無及びその内容」及び「その他参考となる事項」(解説(8)参照)に限られている。これらの事項が全て判明するまで本人への通知をする必要がないというのではなく、本人への通知は、「当該事態の状況に応じて速やかに」行う必要がある。</p> <p>本人への通知については、「本人の権利利益を保護するために必要な範囲において」行うものである。</p> <p>また、当初保護法報告対象事態に該当すると判断したものの、その後実際には保護法報告対象事態に該当していなかったことが判明した場合には、本人への通知が「本人の権利利益を保護するために必要な範囲において」行うものであることに鑑み、本人への通知は不要である。</p> <p>(注) 第2項第(9)号に定める「その他参考となる事項」については、本人への通知を補完するため、本人にとって参考となる事項をいい、例えば、本人が自らの権利利益を保護するために取り得る措置が考えられる。</p> <p>【本人の権利利益を保護するために必要な範囲において通知を行う事例】</p> <p>事例1) 不正アクセスにより個人データが漏えいした場合において、その原因を本人に通知するに当たり、個人情報保護委員会に報告した詳細な内容ではなく、必要な内容を選択して本人に通知すること。</p> <p>事例2) 漏えい等が発生した個人データの項目が本人ごとに異なる場合において、当該本人に関係する内容のみを本人に通知すること。</p> <p>(15)、(16) 同左</p> <p>(参照条文：保護法26条、施行規則7条から10条、通則ガイドライン3-5、金融分野ガイドライン11条)</p>	<p>通則ガイドライン3-5-4-3</p>
<p>第16条～第31条 略</p>	<p>第16条～第31条 同左</p>	
<p>附則 (略)</p> <p>(新設)</p>	<p>附則 (同左)</p> <p>附則</p>	

【新旧対照表】 「個人情報保護指針」

(下線部分改正箇所)

旧	新	根拠法令等
	<p><u>この改正は、令和6年7月1日から施行する。</u> <u>(注) 改正条項は、次のとおりである。</u> <u>第12条、第13条、第14条、第15条</u> <u>を改正する。</u></p>	