個情法(通則編)_自己評価表新旧差分表　　青文字→追加　「ー」→削除

No	ガイドライン項番	大項目	中項目	小項目	条件	確認事項	補足	審査員テキスト	分類		審査			
									規定	運用	必須	該当無	努力	該当無
28	3-5-2	個人データの漏えい等の報告等	漏えい等事案が発覚した場合に講ずべき措置		漏えい等又はそのおそれのある事案（以下「漏えい等事案」という。）が発覚した場合	漏えい等事案が発覚した場合は、その内容に応じて次の(1)～(5)について必要な措置を講じたか。 (1)事業者内部における報告及び被害の拡大防止 (2)事実関係の調査及び原因の究明 (3)影響範囲の特定 (4)再発防止策の検討及び実施 (5)個人情報保護委員会への報告及び本人への通知	(1)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。 (2)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。 (3)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。 (4)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。	【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 事例 6）個人情報取扱事業者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、当該個人情報取扱事業者が、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 【個人データの滅失に該当する事例】 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 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 【個人データの毀損に該当する事例】 事例 1）個人データの内容が改ざんされた場合 事例 2）暗号化処理された個人データの復元キーを喪失したことにより復元できなくなった場合 事例 3）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		★			-	-
30	3-5-3-1	個人データの漏えい等の報告等	個人情報保護委員会への報告	報告対象となる事態	報告対象事態を知った場合	次の(1)～(4)までに掲げる事態（以下「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に報告したか。ただし、「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」が講じられている場合は除く。 (1)要配慮個人情報が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 (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 (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~~当該個人情報取扱事業者に対する行為による個人データ（当該個人情報取扱事業者が取得し、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。）の漏えい等が発生し、又は発生したおそれがある事態 (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	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。 ~~「不正の目的をもって」漏えい等を発生させた主体には、第三者のみならず、従業者も含まれる。~~ 「不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為」（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。また、不正行為の相手方である「当該個人情報取扱事業者」には、当該個人情報取扱事業者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）及び当該個人情報取扱事業者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。 当該個人情報取扱事業者が「取得しようとしている個人情報」に該当するかどうかは、当該個人情報取扱事業者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。 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れば、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。 「個人データに係る本人の数」は、当該個人情報取扱事業者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。	【報告を要する事例】 (1)事例 1）病院における患者の診療情報や調剤情報を含む個人データを記録した USB メモリーを紛失した場合 事例 2）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 (2)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 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 (3)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~~個人データ（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。）が漏えいした場合 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 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 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、当該端末と個人情報取扱事業者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 事例 6）個人情報取扱事業者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、当該個人情報取扱事業者が、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 事例 7）個人情報取扱事業者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、当該個人情報取扱事業者が、当該個人情報取扱事業者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 事例 8）個人情報取扱事業者が、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、当該個人情報取扱事業者が、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 (4)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 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 （ア）~~個人データ~~（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。（イ）において同じ。）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 （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、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 （ウ）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 （エ）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 （オ）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 従業者による個人データ又は個人情報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、個人データ又は個人情報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。		★			-	-
98	3-8-1	保有個人データに関する事項の公表等、保有個人データの開示・訂正等・利用停止等	保有個人データに関する事項の公表等	保有個人データに関する事項の本人への周知	保有個人データを保有している場合	保有個人データの安全管理のために講じた措置は、事業の規模及び性質、保有個人データの取扱状況（取り扱う保有個人データの性質及び量を含む。）、保有個人データを記録した媒体等に起因するリスクに応じて、必要かつ適切な内容となっているか。		当該措置の内容は個人情報取扱事業者によって異なり、本人の知り得る状態に置く安全管理のために講じた措置の内容についても個人情報取扱事業者によって異なる。 なお、当該安全管理のために講じた措置には、個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、当該個人情報取扱事業者が保有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講じた措置も含まれる。		★			-	-