

「個人情報保護法施行規則の一部を改正する規則（案）」等パブリックコメントに対する日本損害保険協会の意見

該当箇所	意見	理由
個人情報保護法施行規則第7条第3号	漏えい報告の対象となる範囲をガイドラインで具体的に明示していただきたい。WEBページの改ざんによるWEBスキミングを規制の対象とすることを目的とした改定であれば、その場面に限定した記載としていただきたい。	個人情報保護法第26条第1項の漏えい報告の対象は「個人データ」に限定されている。これは個人データの漏えい等が生じた場合には、他のデータと容易に結合されること等により、個人の権利利益が侵害されるおそれがあるため、個人情報取扱事業者に対して報告を義務付ける必要性が高いからであると理解している。また、個人情報全般に一律に報告義務を課した場合、個人情報取扱事業者にとって過大な負担を負わせるおそれがあることから、対象が「個人データ」に限定されているものと理解している。この趣旨からしても、報告義務の対象は、個人情報取扱事業者にとって過大な負担とならないレベルまでその範囲を限定し、明確化することが必要と考える。
個人情報保護法ガイドライン（通則編）の一部を改正する告示（案）3-4-2	取得しようとする個人情報全般に安全管理措置を講じることは困難であり、事業者で対応可能な事項に限定していただきたい。	安全管理措置は当該事業者が取り扱う範囲において講じるものであって、取り扱っていない個人情報に対して措置を講じることは困難である。
個人情報保護法ガイドライン（通則編）の一部を改正する告示（案）3-5-3-1	個人情報が含まれるメールを受信した個人情報取扱事業者において、メールシステムがサイバー攻撃にあった場合、メール内に含まれる個人情報は「個人データとして取り扱われることが予定されている」ことに該当するか。	電子メールの本文には様々な個人情報が含まれており、必ずしも個人データとして取り扱うものでないものも含まれている。業として受信したことをもって、「取得しようとしている」または「個人データとして取り扱われることが予定されている」に該当すると解釈される場合、メールシステムがサイバー攻撃の被害に遭うと、メールに含まれるすべての個人情報が漏えいのおそれの対象となってしまうが、その特定、通知は現実的には困難であるため、確認させていただきたい。
個人情報保護法ガイドライン（通則編）の一部を改正する告示（案）3-5-3-1	『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」への該当性は、事例6に示されているとおり「個人情報取扱事業者のウェブサイトの入力ページ」など個人情報の取得を目的としていることが分かるページ等、個人情報の取得が推定される場合に限定されているとの理解でよいか。また、事例6はそのようなページへの攻撃による漏えいを前提としているという理解でよいか。	事例6のように、ウェブサイト自体が「改ざん」される事例だけでなく、DNSサーバの管理アカウントを窃取・窃用され、レコードを改変され、悪サイトに誘導される、という事案も発生している。当該悪サイトについては、個人情報取扱事業者がレコードの改変に気付いた時点では既に削除されており、実際に個人情報の漏えいがあったのか確認できないケースも考えられるため、『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」への該当性は、「個人情報取扱事業者のウェブサイトの入力ページ」等、個人情報の取得が推定されるものに限定されることを確認させていただきたい。
個人情報保護法ガイド	事例6に「個人情報取扱事業者のウェブサイ	個人情報取扱事業者に偽装したウェブサイト

<p>ライン（通則編）の一部を改正する告示 （案）3-5-3-1</p>	<p>トの入力ページが第三者に改ざんされ」について、個人情報取扱事業者に非がないと想定されるケースにおいて、「偽装したウェブサイトの作成」や「廃止したドメインのドロップキャッチによる偽装サイトへの誘導」といった行為により詐取された個人情報は、『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』に該当しないという理解でよいか。</p>	<p>や、既に使わなくなったドメインの悪用について、事前に発見し、予防措置を講じることが困難であり、個人情報取扱事業者に非があるケースでなければ、対策や報告の義務を課すのは困難と思料する。</p> <p>「個人情報の保護に関する法律についてのガイドライン」に関するQ&A 6-6との関連で、Q&Aにも追加説明を記載することを検討いただきたい。</p>
<p>個人情報保護法ガイドライン（通則編）の一部を改正する告示 （案）3-5-3-1</p>	<p>事例7に「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」とあるが、「偽の入力ページに入力した個人情報が第三者に送信されたかどうか」確認ができないケースは報告不要との理解でよいか。</p>	<p>「偽の入力ページに遷移した」ことまでは個人情報取扱事業者側で、ログで判明する可能性はあるが、「偽の入力ページに入力した個人情報が第三者に送信されたかどうか」は調査できないケースも多いと考えるため、確認させていただきたい。</p> <p>なお、「偽の入力ページに個人情報を入力した」本人（被漏えい者）から、不審メール他の被害の申告がある場合は、第三者に送信されたものとして報告対象に該当すると考えている。</p>

以上