

「個人情報保護法施行規則等の改正」および「被害報告一元化に関する DDoS 事案及びランサムウェア事案報告様式」(案) に対する日本損害保険協会の意見

No.	該当箇所	意見	理由
1	個人情報保護法施行規則 第 8 条第 3 項	委託先による漏えいの場合、委託先と委託元双方が「ランサムウェア事案共通様式」を使用して報告書を作成する必要があるか。委託先が攻撃の対象になり、委託元において特段警察への相談等を行わない場合に、委託元が作成すべき報告書様式を確認したい。	左記のとおり。
2	個人情報保護法施行規則 第 8 条第 3 項	今回の改正以後は、被害組織となった保険代理店または外部委託先は共通様式を用いた漏えい等報告を行うことに加え、委託元保険会社は、保険代理店または外部委託先から「ランサムウェア事案共通様式」による通知を受けそこから改正前と同様の漏えい等報告を行う必要があるとの認識で良いか。	従前より、個人情報保護法第 26 条第 1 項ただし書きにより、被害組織となった保険代理店または外部委託先からの通知を受けて、委託元である保険会社が漏えい等報告を行っているが、この対応に何等か影響があるのかを確認したい。
3	個人情報保護法施行規則 第 8 条第 3 項	今回の改正以後も、委託元としてこれまでと同じ様式での報告は引き続き許容されるとの認識で良いか。 もし許容されない場合、速報後にランサムウェア被害と判明した事案について、確報では「ランサムウェア事案共通様式」に切り替えて報告する必要があるのか。	従前より、個人情報保護法第 26 条第 1 項ただし書きにより、被害組織となった保険代理店または外部委託先からの通知を受けて、委託元である保険会社が漏えい等報告を行っているが、この対応に何等か影響があるのかを確認したい。
4	ランサムウェア事案 共通様式	「ランサムウェア事案共通様式」では、内閣サイバーセキュリティセンターへの共有等を希望しない選択が可能となっているが、当該希望をしないケースとしてどのような場面が想定されているか。	「ランサムウェア事案共通様式」で設定された設問の趣旨を確認したい。
5	ランサムウェア事案 共通様式	「ランサムウェア事案共通様式」冒頭にある「2. ランサムウェア感染時のお願い」において、初期対応のみならず例えば以下のような形で復旧までの対応を記載いただきたい。 また、現時点で初期対応についてのみ記載されている背景について、ご教示いただきたい。  「封じ込め（被害拡大防止）」	ランサムウェア感染時においては、初期対応のみならずその後の対応においても速やかな対応が必要であり、その明示をすることで被害組織の対応が円滑となると考えるもの。

No.	該当箇所	意見	理由
		<ul style="list-style-type: none"> <li>・感染が疑われる機器類を速やかにネットワーク（有線・無線）から切り離すこと</li> <li>・感染が疑われる機器類や、当該機器類からアクセス可能なシステム（特に個人情報を含むもの）について、認証情報の変更または一時的なアカウントロックを実施すること（ネットワークから切り離してしまい対応不可の場合は、復旧時に対応すること）</li> </ul> <p>「証拠保全」</p> <ul style="list-style-type: none"> <li>・後続の詳細な調査（フォレンジック調査）において、十分な調査をするために証拠保全をする必要がある。以下の操作を行うと、証拠が保全できない可能性がある。 <ul style="list-style-type: none"> <li>-感染端末等の再起動や電源オフ、既に感染端末等の電源がオフの場合はオン</li> <li>-ウイルス対策ソフトによる感染端末等のフルスキャン</li> <li>-ネットワーク機器の再起動や電源オフ</li> <li>-ファームウェアや OS のアップデート</li> </ul> </li> </ul> <p>「フォレンジック調査」</p> <ul style="list-style-type: none"> <li>・ランサムウェア攻撃に関する詳細な調査（フォレンジック調査）は、自社のみでの対応は困難であるため、信頼できる外部の専門機関に依頼すること。</li> </ul> <p>「接続再開方針策定・復旧」</p> <ul style="list-style-type: none"> <li>・フォレンジック調査の結果をもとに根本原因を特定し、再発防止策を策定したうえで、自社および接続先の合意を得てからネットワーク接続を再開すること。</li> </ul>	