資 料 4

平成 27 年 8 月 6 日会議資料

中 間 サ ー バ ー に つ い て

～　国（総務省）への確認事項　～

特定個人情報保護委員会規則第７条第４項の規定に基づき実施した第三者点検において、全項目評価書案に記載した中間サーバーに係るリスク対策等の記載内容(「特定個人情報保護評価書の作成の際に必要となる中間サーバーに関する情報の提供について　平成２６年８月８日　総務省個人番号企画室長」から引用したもの）が、情報セキュリティ対策の観点からリスク分析が不十分ではないかとの意見をいただいています。

そのため、それらの意見に対する見解をお示しいただくとともに、下記についてご協力いただけるようお願いします。

１　地方公共団体情報システム機構が中間サーバーに関する記載例を作成するにあたり、実施した評価結果やリスク分析の結果等について情報提供していただきたい。

＜ 国の回答 ＞

リスク分析については､セキュリティの観点でのリスクの洗い出しとその対策を検討しております。

なお、個人情報保護評価の記載例については個人情報保護委員会において内容の適合性・妥当性について評価が行われております。

２　地方公共団体システム機構が作成した中間サーバーに関する記載例には､不正な利用を未然に防止あるいは被害の拡大を防止するための対策としてアクセスログ等を記録するとあるが､記録した情報をどのように活用して対策（例えばアクセスログを定期的に監視する仕組みを整備）を行うのか、についての記載がないことから､「ベネッセの個人情報漏えい事件が考慮されていないのではないか」との意見があったため、今後、必要に応じて記載例を更新していただきたい。

＜ 国の回答 ＞

自治体中間サーバー・ソフトウェアとしてはアクセスログをＣＳＶファイルとして出力する機能を設けており、ログファイルをどのように扱うかについては各団体の運用によるものと認識しております。各団体において必要な措置をご検討いただきたいと考えております。

【第三者点検における主な意見】

（1）どのようなリスク分析を行った結果、このような記載例に至ったかという、バックデータを国に示していただきたい。

＜ 国の回答 ＞

別紙「脅威と対策」のとおり

（2）【記載例 P2 「Ⅱ 特定個人情報ファイルの概要」】－「6 特定個人情報の保管・消去」－「③ 消去方法」について

「中間サーバー・プラットフォームにおける措置」の①で、「通常、中間サーバー・プラットフォームの保守・運用を行う事業者が特定個人情報を消去することはない。」と記載されているが、「通常でない場合」のリスクの記載が不足している。

②の事業者によるハード更新等による消去が「通常でない場合」の一例と思われるが、この他にも、例えば、プログラムの不具合等により、事業者が直接ハードウェアにアクセスして作業をする場合、保守・運営上、特定個人情報の消去に至る可能性が考えられるが、このようなリスクについて、どのような対策を行うのか。

また、「ディスク交換やハード更改等の際は、中間サーバー・プラットフォームの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。」と記載されているが、「完全に消去した」ことを確認（最低限、証明書を受領する等）するのか。

＜ 国の回答 ＞

①データベースに係る機器において作業を行う際は、作業前にバックアップを取得する想定であること。

②なんらかの事由により、作業中に副本データが失われた場合は、そのバックアップデータによりリストアを実施することを想定していること。

③特定個人情報の格納されるデータベースは暗号化されているため、ハードウェアから直接アクセスされても特定個人情報にアクセスはできない設計となっていること。

④ハードディスク交換などを行う際は、物理破壊を原則にデータ消去を行い、その証明書を受領する想定であり、その方法等については現在Ｊ－ＬＩＳにおいて運用設計中であること。

（3）【記載例 P3 「Ⅲ 特定個人情報の取扱いのプロセスにおけるリスク対策」】－「6．情報提供ネットワークシステムとの接続」－「リスク１：目的外の入手が行われるリスク」について

「中間サーバー・ソフトウェアにおける措置」の①に「番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。」と記載されているが、成り済ましによる照会に対してのリスク対策が記載されていない。

＜ 国の回答 ＞

別紙「脅威と対策」のとおり

（4）【記載例 P3 「Ⅲ 特定個人情報の取扱いのプロセスにおけるリスク対策」】－「6．情報提供ネットワークシステムとの接続」－「リスク１：目的外の入手が行われるリスク」について

「中間サーバーソフトウェアにおける措置」の②に「中間サーバーの職員認証・権限管理機能（※3）では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、捜査内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を防止する仕組みになっている」と記載されているが、ベネッセの個人情報漏えい事件を考慮すれば、アクセスログをとっているだけではリスク対策として不十分であり、未然に防止あるいは被害の拡大を防止するためには、アクセスログを定期的に監視する仕組みが必要である。

＜ 国の回答 ＞

ログファイルをどのように扱うかは各団体の運用によるものであり、各団体において必要な措置を検討していただきたい。

（市政情報室：これにつきましては、情報関係の課と記載内容等を早急に協議し、次回以降の部会において、その対応策をお示ししていきたいと考えております。）

（5）「中間サーバーに関する特定個人情報保護評価の実施に当たって」（平成２６年８月総務省大臣官房企画課個人番号企画室）のＰ７に、「特定個人情報ファイルは、各地方公共団体が自ら管理することとしていることから、特定個人情報ファイルの取扱いの委託と取り扱っていない。」と記載されており、中間サーバー・プラットフォームはクラウドサービスの形態となると思われるが、番号法の罰則は適用されるのか。

また、クラウドサービスを提供し、データベースを管理するJ-LIS（地方公共団体情報システム機構）と地方公共団体はどのような関係あたるのか。

＜ 国の回答 ＞

①中間サーバー・プラットフォーム上にある中間サーバーに格納される副本データは、あくまで地方公共団体がその内容について管理するものであること。

②なんらかの事由により、地方公共団体の副本データが失われた場合、バックアップデータによりリストアを実施する、もしくは地方公共団体により、再度副本データを登録していただくことを想定していること。

③番号法の罰則については、総務省は判断しかねるものの、少なくとも、地方公共団体とＪ－ＬＩＳは、サービス利用者とサービス提供者との関係であり、委託と受託の関係でないこと。