

- 1 日 時 令和8年7月31日（金） 9：15～9：55
- 2 場 所 愛媛県庁第2別館 10階 1004会議室
- 3 出席者 光信会長、牧本委員、長尾委員、森本委員、小林参考人
- 4 次 第
(1) 開会
(2) 議事

ア 特定個人情報保護評価書

- ・資料に基づき、税務課から説明。

[委員の主な意見]

- ① 重大事故の「発生あり」に関して、県は委託先のセキュリティ等をどう把握し、それが十分かどうか、不十分ならこうしてほしいといった働きかけはあるのか。→委託する際は、事業者の個人情報の取扱いについての管理体制や、例えば、従業員への教育、物理的にこういうシステムを使っているのに漏れないといったセキュリティに関することなどを事前に提出させている。
- ② 前回5年前は「評価書に対する意見」が2つあったが、どう対応したのか。→1点目の「データ消去の確認」については、文言と図の記載方法をわかりやすい表現に修正。2点目の「評価書の記載方法」は御指摘どおり修正。
- ③ 1点目について、誰がどのような方法で消去したのか、消去したことを誰が確認したのかということを、きちんと後から検証可能な状態にしてあるのか。→実際その作業を行った時は、その都度、実績報告をもらう約束をしている。
- ④ NTTデータがリスク事案に係る事業者なのか。→違う。システムを保守していたNTTデータではなく、県税の納税通知書の印刷を委託していた事業者から情報が漏れたということ。本来、委託先が手順どおりにしていれば、ネットワークが遮断されているので誤謬がなかったが、従業員の手間とか、そういうのを簡略化するため、インターネット環境の中で作業してしまったもの。
- ⑤ サイバー攻撃などの外部からの攻撃に対する対策は、評価書のどこに記載があるのか。→外から通信できないような仕組みをスマート行政推進課で構築した中に、県税システムや、マイナンバーを使うような情報システムも入っている。直接、外から攻撃されることはない。
- ⑥ 物理的な破壊に関し、立ち会うのは、非正規ではなく正規職員に限定、と明記したほうがいいと思う。

[小林参考人の意見]

- ⑦ 13ページ「④入手に係る妥当性」の「紙」でのやりとりは、このページだけでなく他にも何ヶ所かあったと思うが、使い終わった紙、不要になった紙の処分方法について記載した方がいい。紙として残るのは情報漏えいの一つの原因になるので、具体的な作業としての処分方法だけでなく、処分したことの確認の記録、いつ、どのようにやったのかという記録をしっかりと残しておくことが重要ではないか。やっているなら、その状況を明記した方がいい。
- ⑧ 同じ④の最後の「電子記録媒体により入手」について、従来からUSBメモリーに正規でないものが紛れ込む危険性は認知されていたが、最近、自衛隊のUSBの問題もあったので、具体的にどういう電子記録媒体なのかが気になる。USBメモリーだけでなく、ハードディスクなどの外付けの記憶メディアも含

め、正規かどうか確認したものを使用する手順が必要ではないかと思う。加えて、プリンターは大丈夫だろうと思いがちだが、そういったものの中にも、ワーム、マルウェアが仕込まれる可能性は実はゼロではない。おそらく県税クラウドサービスからぶら下がるプリンターは、ちゃんとしたところから購入されていると思うが、一応そういうことを確認すべき。インターネットから切れているから、といって、安心せず、しっかりパッチをあてる等してほしい。また、今のプリンターは印刷データを残しており、後で他の人が印刷できる機能があるので、設定変更等をしっかりとやって管理する必要がある。ネットワークに繋がるあらゆるものが、そういうことをやりかねないのが今の時代だと、意識していただければと思う。

- ⑨ 15ページ②の中の「その妥当性」の二文について、「県税クラウドサービスの安定的な稼働のため、専門的な知識を有する民間事業者にシステムの運用維持管理を委託する必要がある」というのは、主語は「県」で、次の文章を読むと、「その運用維持管理を実施するために、特定個人情報ファイルを含むシステム全体で取り扱う必要がある」とあり、これは主語が「委託先」。文章自体は県が何をするかという文章なので、「県が」はいちいち入れなくてもいいが、後半部分は、委託先がやるべきことなので、「委託先は」といった表現は入れた方がよい。
- ⑩ 19ページ「①保管場所」の「県税クラウドサービスにおける措置」の2番の「入口扉は生体認証を採用している」について、入口のことは述べているが、セキュリティレベルの高いところは、入退室のペアの管理をするケースがある。出ていくのを管理しないと、その人がまだ残っているのか、いつ出たのかわからない。そうすると何かあったときに、誰がいるときに起こったのかが全然わからなくなる。入退室を必ずペアで管理し、退室手続きをしなかった人は次は入れないというような管理をするべきではないか。29ページの「具体的な対策の内容」の「サーバー室の入り口扉は生体認証」も同様。
- ⑪ 23ページ「アクセス権限の管理」の「具体的な管理方法」で、「システムパスワードは、定期的に変更する」について、他も何ヶ所か「定期的」という言葉が出てくるが、「定期的」の周期に言及すべきではないか。1ヶ月ごととか3ヶ月ごととか、具体的な期間の表現にした方がいいと思う。これは他のところも見直してほしい。
- ⑫ 23ページ「リスクに対する措置の内容」の2の最後の「適切に処理したことを確認する」について、先ほどの委員の御指摘のとおり、誰が確認するのか、確認した結果の記録は残すのか、ということを実際にはやっていたいていと思うが、そこまで言及した方がいいと思う。
- ⑬ 24ページ「情報保護管理体制の確認」の「委託事業者の個人情報管理体制等を確認する」について、これ自体はいいが、委託業者に体制の変更、組織の変更があった場合、ちゃんと県に報告されるようになっているか、あるいは、変更には承認が必要という条件をつけてもよい。もちろんそれを実際にさせることが大事で、やっているならそれでいいが、変更に対し適切に対応していることがわかる記述を入れるべき。
- ⑭ 同じページ「特定個人情報の消去ルール」の「ルールの内容」の2番目「委託先自らが収集し、又は作成した個人情報記録された資料等は、業務完了後速やかに、かつ確実に廃棄又は消去する」について、県が委託業者にどの

ようにやらせて、どう把握、管理しているのかを記載する必要があると思う。

- ⑮ 28ページ「外部記録機器媒体を利用する場合は、使用する媒体を限定する」は、先ほど申し上げたとおり、USB等の媒体を使う場合は、それに偽物が紛れ込まないかということを適切に確認していただきたい。
- ⑯ 32ページ「従業者に対する教育、啓発」の「具体的な方法」の「愛媛県における措置」で、「年1回研修を実施」、「セキュリティ研修を実施」とあるが、研修の形骸化がちょっと心配。至るところでそういう話があるので、「研修やりました」ではなくて、やった結果として受講者に内容が定着しているかという効果測定を実施すべきと思う。研修直後の効果測定とか、年一回の研修なら半年後に、とか、そういったことをする必要があると思う。実際にしているのであれば、それを記載してはどうかと思う。

[まとめ]

次回審査会において、意見の取りまとめを行う。

※公開部分は以上