地方公共団体における情報セキュリティポリシーに関する
ガイドラインの改定等に係る検討会（第７回）

日　時：令和５年１月 12 日（木）13:00～14:00
形　式：オンライン会議
議　事：
１．「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定案について

○：構成員　●：総務省（事務局）

資料１　地方公共団体における情報セキュリティポリシーに関するガイドライン改定のポイントについて①（クラウド利用関係）

○13 ページの組織体制に関連して、内部監査の体制を伺いたい。

●内部監査については、監査ガイドラインをお示ししており、監査人を指名して監査を実施することを想定している。

○監査ガイドラインに反映するということであれば、13 ページの図にも反映する必要があるか検討いただきたい。

●承知した。なお、13 ページの図は、クラウドサービス利用における組織体制として新たな役職を任命するのではなく、既存の体制を踏襲して対応することを想定している。

○地方公共団体が混乱しないよう、説明いただいた意図を資料にも示していただきたい。

○13 ページの図について、クラウドサービスの SaaS 利用が進むほど職員がコントロールできる範囲が限定されてしまい、現在のオンプレミス運用よりも事業者に依存する体質となってしまうことを懸念している。クラウドサービスで事故が発生した場合に、地方公共団体が委託元の責任を放棄してしまわないよう、監査の重要性を記載すべきである。

●クラウドサービスの場合、ユーザーによってはオンプレミスに比べてシステムやデータの管理が事業者に依存しやすくなる面があるということは、承知している。ガイドライン改定案においても、契約による責任範囲の明確化及び監査の重要性は示しているところであるが、ご指摘を踏まえ、地方公共団体に伝わりやすい内容となるよう検討したい。

○デジタルフォレンジックの観点で、クラウドサービス側では様々なデータを取得しているが、地方公共団体が公開を求めた場合に、契約段階で契約に明記しなかったために、ベンダから開示されない場合がある。そのような事態に備えて、契約の段階、監査の段階で具体的にどのような対応が必要か詳しく示すことを検討いただきたい。

●承知した。

○15 ページの LGWAN 接続系でのクラウドサービス利用について、β’モデルの場合、個々の端末を守るためにはゼロトラストに近い考え方が必要になると考えられる。今後、自治体情報セキュリティクラウドについて、境界型防御で十分なのかの検討が必要ではではないか。

●令和２年度のガイドライン改定でβモデルについて認めたところであり、２年程度経過したところである。全国の地方公共団体の状況を確認すると、都道府県や政令指定都市では、βモデルに移行している団体もあるが、全体として多くの地方公共団体では、αモデルを採用している団体が多数であり、現状の分析を踏まえて検討していきたい。また、自治体情報セキュリティクラウドは、現在、第 2 期の運用を各都道府県で行っていただいているが、次期の検討では、境界型防御を前提とした対策で十分なのか、ゼロトラストに近い考え方が必要なのか等について検討してまいりたい。

○12、13 ページのクラウドサービス利用における組織体制に関連して、クラウドサービスで障害が発生した場合、個別団体のみならず広域に複数の団体に影響が波及し、対応を迫られることが考えられる。その場合、国が窓口となって事業者と連携して対応いただくことはできないか。複数の自治体に影響のあるインシデントの連絡や対応の体制を検討いただきたい。

●13 ページの図は、地方公共団体の庁内の組織体制を示したものであるが、地方公共団体、事業者及び外部との連携体制については検討したい。なお、ガバメントクラウドについては、デジタル庁がインシデント発生時の連絡体制について検討中である。ガバメントクラウド以外のクラウドサービスで事故が起きた際については多くの地方公共団体が利用するクラウドサービスの場合には、必要に応じて総務省が事業者に状況をヒアリングし、地方公共団体に情報提供を行う等の対応を検討したい。

○11 ページの個人情報保護法との関係について、地方公共団体の負担を軽減できないかという観点で、体制面、制度面から個人情報保護委員会と協議いただきたい。

●個人情報保護委員会と連携して対応していきたい。

資料２　地方公共団体における情報セキュリティポリシーに関するガイドライン改定のポイントについて②（情報セキュリティインシデント関係）

○セキュリティポリシーガイドラインの改定において、外部委託先管理の内容を補強するのは妥当である。しかし、根本的には委託管理するための知見や能力が尼崎市に欠けていたことが真の原因でないか。外部委託先管理における具体的な取組の例示も重要であるが、委託する側にどのような知見や資質が要るかを示すことも必要。

●外部委託先管理は、契約で責任分界を定めることに加えて、今回新たにチェックリストで確認を行っていただくことを考えている。地方公共団体の知見、デジタル人材の育成といった観点では、総務省においてデジタル人材支援を行っているところであり、今後どのようなことができるか検討していきたい。

○職員の教育や力量の評価は難しいので、今回、チェックリストで仕組化を図ることは効果的であると考える。

○チェックリストは、データの持ち出しに関する内容に偏っているように見受けられる。今回の問題が情報漏えいのため、その部分を中心にするのは分かるが、尼崎市の事例では、システムのテストにおいて本番データを使っていたことが問題であった。他の地方公共団体でも同様に、委託先事業者からテストにおいて本番データを使用したいと言われて許可してしまう危険性がある。そのような対応は問題であると気付きを促せるように明確にするべきではないか。

●テストの際は、本番データを使わないという観点が抜けているため、ご指摘いただいた点について、記載の追記を検討したい。

○J-LIS の地方公共団体向けの研修は、総務省と連携の上、最新の動向が反映されているか。

●研修資料の内容について、総務省でも事前に確認するなど、J-LIS と連携している。引き続き連携して研修内容に反映していきたい。

以　上