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９回）

開催日時：令和５年 10 月 10 日（火）13:15～15:05
開催場所： オンライン会議
議　　事：
１． 地方公共団体情報セキュリティ対策の経緯について
２． 本検討会の検討事項及び検討の方向性について

○：構成員　●：総務省（事務局）
１．地方公共団体情報セキュリティ対策の経緯について

（意見、質問等なし）

２．本検討会の検討事項及び検討の方向性について

○政府統一基準における機密性３情報は、最も機密性に配慮すべき情報として個人情報が扱われている。総務省では、令和２年の通知で「住民の個人情報、職員の個人情報等の非公開情報」と記載しているが、地方公共団体の実情は、住民の個人情報が必ずしも非公開とはなっていない。また従来の使い方としては、職員の個人情報はLGWAN接続系に置かれ、住民の個人情報はマイナンバー利用事務系に置かれる等、分けている。また、機微性が高い情報は管理方法が異なるため、総務省ガイドラインに、すべての個人情報を機密性３にすると記載してしまうと、範囲が広くなりすぎてしまうということを懸念している。

●令和２年度の地方公共団体への通知では、すべての個人情報を機密情報３とするのではなく、その内の非公開情報という枠を設けたことが大きなポイントになる。また、すべての個人情報を機密性３情報として扱うと業務に差しさわりがあるため、機密性の分類の記載については、個人情報の種類に留意した上で、次回に案を提示する。

○小規模の地方公共団体は、契約や契約後の管理はベンダーに任せきりになりがちで、職員自らが管理するリソースは不足していると考える。そのため、契約上の注意点や契約した後にベンダーへの要求事項を具体的に分かるようなガイドラインの記載を検討する必要がある。

●小規模でリソース不足の地方公共団体こそ契約時に留意し、個人情報が流出することを防がなければならないため、記載について検討していく。

○αモデルにおけるローカルブレイクアウトについて、接続先がどこかが重要であり、ローカルブレイクアウトの接続先を限定することが必要である。
○更にクラウドサービスの利用が進むとクラウドサービスに対するデータの流れを含めた監視も

考える必要がある。

●ローカルブレイクアウトの接続先の考え方については、リスクアセスメントを踏まえ案を提示する予定。
●ローカルブレイクアウトで使用されるクラウドサービスの監視についても、リスクアセスメントの結果を踏まえて提示できればと考えている。

○機密性のラベリングについて、NISC と地方公共団体で同じラベリングをしているが、内容が異なるため、同じ言葉を使うと現場に混乱を招くことが懸念される。現場で区別が付くように検討すべきである。
○数字を使うこと自体が悪いのではなく、中央省庁（政府統一基準）と同じ表記だけでは混乱が起こると考えている。そのため、例えば「自治体」を「機密性３情報」の頭あるいは間に付ける等で、ラベリングを区別しやすくすればよいのではないか。
○住民情報と職員情報を分けるべきとの意見は賛成である。

●数字で分類している理由としては、３が最も機密性が高く機密性に配慮いなくてはならない、１は最も軽い情報ということを数字の大きさで瞬時に区別できることと、３段階で分類すると最も整理しやすいため、このような基準を設けている。
●ご指摘のとおり、国の統一基準とガイドラインの機密性の分類や基準が分かりやすいように、ガイドラインの中では「自治体」の用語を機密性分類の名称に付けるといった方法もあると認識した。

○クラウドサービス利用可否の判断基準に用いるのであれば、機密性レベルを２と３で分けるのか、国でいう機密性２とするのかは非常に重要な点である。
○職員情報と住民情報は分けた方がいい。
○今後、ガイドラインで例示するとのことだが、台帳は機密性３だと考えているが、電子申請のトランザクションデータのように個々に発生するものは機密性２に該当するのではないか等、クラウドサービスの利用促進を妨げないような例示が必要。

○令和２年にβ’モデルが出た時に、将来的にはインターネットに接続するシステムか、保護すべきシステムかの２層に分けていくことを目指していると思っている。そのため、β’モデルに多くの地方自治体を誘導するということに対して賛成である。
○一方で、基礎自治体は、LGWAN-ASP が非常に普及している。β’モデルにすぐ移行できない自治体もあるため、α’モデルを検討することは賛成である。
○個人情報は機密性が高いためクラウドサービス利用ができない等、地方公共団体の中では思考停止になっているところがある。人事情報と一般的な住民情報を分けることや、文部科学省のガイドラインを参考にする等、個人情報を一律に機密性３としないことも大事ではないか。
○地方公共団体が自治体 DX に取り組んでいる中で、マイナンバー利用事務系のパソコンしか配付されていない職員は電子決裁やコラボレーションといった新しい動きに取り残されてしまっている。総務省が進めている自治体 DX ともかけ離れてしまうと感じているため、画面転送に

ついて２年を掛けて慎重に検討することは賛成する。

●個人情報の分類については、文部科学省のガイドラインも参照しつつ今後の検討を進めていきたい。
●画面転送は、政令指定都市などから要望を受けているが、小規模団体からも切実な利用の希望があることを認識した。リスクアセスメントも含め、慎重に検討を進め安全な方法を提示していく。

○マイナンバー利用事務系の画面転送は、リスクアセスメントを実施し安全性を確認した上で対応しないと問題があり、何か起こった時の影響が大きいと考える。リスクアセスメントを実施することを前提に、少し時間を掛けてもよいので安全性を確認してからやるべきである。

○政府が示すインシデントが起こることを前提に被害を最小限に抑えるというゼロトラストの考え方に従うと、個人情報は漏れる前提といった問いが生じる。そのため、政府が示すものをそのまま採用することは危険である。
○ローカルブレイクアウトは、接続先以外との通信がないため安全という考え方であるが、アップロードやコミュニケーションツール上でファイル添付ができるため管理は必要である。
○業務で使用しているコミュニケーションツール等は、特定の通信を止めると使えなくなることが分かっており、GAFAM の通信先であっても安全とは限らない（インターネットに直接繋いでいるリスクとあまり大差がない）ため、気を付けなくてはならない。

●ISMAP に登録されているクラウドサービスであっても 100％安全ではないことは理解しているが、資料２－１で説明したように、自治体がよく使用しているサービスがクラウド化される中で、自治体がインターネットを更に利用していかなくてはならない状況に変化していると考えている。少しでもリスクを軽減していくことができるよう、検討を進めていきたい。
●マイナンバー利用事務系は、境界型防御でインターネットには晒さないというのが１つ大きな考え方としてある。その上で、インターネット接続系等の業務端末については、β’モデルを使って対策を講じられるよう、方針を検討していきたい。
●ローカルブレイクアウトについては、今後検討会でリスクアセスメント結果を踏まえて改定案を提示する。

○小規模自治体では、β’モデルへの移行を検討したことがないとあるが、どのようにすれば検討してもらえるかを研究する必要がある。おそらく移行・導入コストや移行を検討するコストが大きく見えていると思う。
○地方公共団体はガバメントクラウドを気にしており、どのタイミングで何を検討すればいいか等、今後、情報が不足している部分を懸念点として挙げられるのではないかと思われる。そのため、全体的に情報提供が大事と考えている。
○次期 LGWAN や標準化が同時並行で動いている中で、令和５年度のガイドライン改定の進め方について、どのタイミングで何が行われ、何が論点となっているか、地方公共団体側に立って細かい分かりやすい見せ方が必要なのではないだろうか。長期間のなるべく具体的なロードマッ

プ、スケジュール感を提示してほしい。

●β’モデルへの移行支援については、費用面の補助が難しいため、移行事例の横展開や、手順書などで具体的に示すことにより、コスト以外での支援を考えている。ただし、ネットワーク更改のタイミングによってはβ’モデル移行が難しいため、そのような自治体に対しては、ローカルブレイクアウトのモデルを提示することで対応していく。
●ガバメントクラウドの対応については、デジタル庁と連携を図っていく。またβ’モデルなど、ガイドラインのネットワーク構成に関する部分は、今後自治体に参考にしていただくものとして提示するもので、即座に機器購入などの対応の必要があるものではないことにご留意いただいた上で、地方公共団体に周知していければと考える。

○個人情報の機密性に配慮すべき情報として扱うことへの方向性に異論はない。
○個人情報だから大事という思考停止的な発想ではなく、使われ方がもたらすリスクを考えた上で重要性が高いと判断すべきと考える。ただし、ガバメントクラウドの利用対象外なのか否かで取り扱いが変わってくるため、地方公共団体の現場で困らないようにより具体的に方向性を示すべきではないか。

●ご指摘の通り、情報の性質、用途などに注意して案を検討していく。

○β’モデルの推進について、なぜ三層に分けたかの議論を踏まえると、αからβに移行することによってセキュリティを緩める方向になることから、後ろ向きになってしまう地方公共団体が出るのは明らかである。またβ’モデルは、運用コストが高いため、小規模自治体には、β’に移ろうという気が起こらない場合も少なくない。β’モデルの推進ありきにならないように議論を進めてほしい。
○機密性区分について、NISC の政府統一基準は地方公共団体も大枠では沿っているという前提がある。そのため、定義が変わることによって齟齬が発生し、自治体の情報システムが政府統一基準を満たしているか否かの議論になりかねないことを指摘しておく。
○コンビニ交付サービスに関する事案に対する対策として、サービス選定をする際、J-LIS の受入れに関する基準を明確にする等、地方公共団体への負荷が軽減される仕組みを考えていくことが必要である。
○ローカルブレイクアウトは、地方公共団体にてなし崩し的に推進されていることに危機感を持っている。まず LGWAN という仕組みを活かして改善していくという方法があるのではないか。
○LGWAN はかつてトンネルとして使われた実績もあり、UDP であることが問題だとは思えない。機能が足りないのであれば LGWAN 側で対応するべきだと思う。

●ご懸念について理解。クラウドサービスの利用といった業務効率化の観点だけでなく、三層の対策に至ったセキュリティの観点や、地方公共団体の負担を考慮し、必要に応じて関係箇所と調整しつつ検討を進める。

○個人情報の考え方にて、全住民を集めている台帳と住民から個別に申請が来る情報、住民情報

では、長時間使うシステムと短時間で終わるシステム等で考え方を変えることにより、クラウドサービスをより活用できると思うため、ガイドラインに記載されていると良いのではないか。

○マイナンバー利用事務系と接続が可能なインターネット系サービスについては、ガイドライン上で eLTAX かマイナポータルが限定と挙がっているが、限定的にするか、どこまで対策を講じていれば可能であるかを明記すると良いのではないか。

○コンビニ交付については、J-LIS 等がどこのパッケージソフトであれば大丈夫である等の保証する形がとれると、地方公共団体としてはコンビニ交付サービスを利用しやすくなるのではないか。

●ご指摘を踏まえ、必要な調整を行った上で、改定案を提示する。

●次回は、11 月下旬から 12 月上旬での開催を予定している。日程は改めて調整し、連絡する。

以上