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15回）

議事概要　要旨版

開催日時：令和６年 11 月 27 日（水）13:15～15:15
開催場所：オンライン会議
出席者：（敬称略、五十音順）

議　　事：

１．番号法関連規定を踏まえたマイナンバー利用事務系に係る画面転送・無線 LAN 利用について
２．マイナンバー利用事務系に係る画面転送について
３．政府機関等のサイバーセキュリティ対策のための統一基準群の改定に伴う対応

○：構成員　●：総務省（事務局）

１．番号法関連規定を踏まえたマイナンバー利用事務系に係る画面転送・無線 LAN 利用ついて

○ 今後政令市などでは本庁舎から区役所へ移動し仕事するケースが増えると考えられる。端末を「執務エリア」から移動させないルールについては、もう少し柔軟な運用を考えていただきたい。

● 支所等は「執務エリア」に含めている解釈である。「執務エリア」については、各団体で定義し、担当者がその範囲内でマイナンバーを確認することを検討している。

○ 単に「事務取扱担当者の端末は移動させない」という書き方では担当者になった以上、その担当者の端末は全て持ち出すことができないと誤解を招く恐れがある。その点を明確化していただきたい。

● 「事務取扱担当者」は番号法上の安全管理措置に基づく用語であるため、その定義を明確にする形で改定案を示すようにする。

○ 執務室以外に持ち出さないのであれば、有線 LAN のみに制限することと同義ではないか。

○ 執務室の中でしか接続ができないよう SSID を設定し、SSID 接続時はマイナンバー利用事務系の事務が行えるようにすることで、端末認証という技術的対策で縛ることもできるのではないか。

● 現行のように有線のみで運用する場合、断線のリスクがあると聞いている。無線 LAN をマイナンバー利用事務系まで含めて認めることで、負担軽減だけでなく有線 LAN の断線による可用性の阻害も防ぐことができると考える。

２．マイナンバー利用事務系に係る画面転送について

○ 例えばDaaSがどのような機能を持っていれば問題がない等、用語の前提条件を明示していただきたい。前提条件が明示されていないと、安全性が担保できないDaaS等が入ってくる余地があると考える。

○ ISMAPの登録業者、いわゆるCSPが提供するアプリケーション等が全てISMAP準拠というわけではない旨が伝わるよう記載を工夫していただきたい。

● 用語については、自治体の誤解を生まないような形で定義を示すことを検討する。

○　既にオンプレミスのVDIでLGWAN接続系からマイナンバー利用事務系にアクセスしている団体数は全国的に結構な数であると考えられ、スクリーンショット機能を停止した際はハレーションが起こると思われる。

● 利便性が阻害されるという観点で、ハレーションがあることは予想できるが、スクリーンショットで情報を窃取されるリスクについて、学識者から問題視されている。このようなリスクに対する考えがあれば伺いたい。

○ 画面転送自体リスクが高いと考えるため、まずは必要な対策を列挙し、使い勝手とのトレードオフで対策の順位付けをする議論が必要と考える。

○ マイナンバー利用事務系をDaaSで利用する際は、LGWAN接続系に画面ハードコピーが誤って利用されないような対策が必要と考える。例えば、DaaSのランチャーに対してLGWAN接続系とマイナンバー利用事務系で別の設定を施す等の技術的な対策を行う必要があると考える。

○ 人的な対策として不要なサイトへのアクセス等に対する、自治体内の懲戒ルールはガイドラインに今後記載することはあり得るのか。

● ガイドラインはあくまでもセキュリティの対策について示したものであることと、自治体職員への懲戒処分については、個別の事案に応じて考えられるべきものであるため、別の論点として整理すべきと考えている。

○ 標準化対象業務のシステムの実情はいわゆるマルチクラウドになっており、多くは AWS を使用しているが、一部システムは別の CSP 上に構築している自治体もある。そのあたりは想定された図であるか。

● 図では簡略化されているが、想定している。

３．政府機関等のサイバーセキュリティ対策のための統一基準群の改定に伴う対応

○　IoT 製品のセキュリティ適合性評価制度の「☆1」「☆2」については自己宣言レベルであるため留意すべき。

○　重要インフラのサイバーセキュリティレベルを上げる政府の動きに合わせる形で、政府統一基準群が改定されると自治体にも影響してくる構図となっている。段々と、小さな自治体の身の丈に合わない要求になることが懸念される。

●　「☆」のラベルを確認することを、その「☆」取得に求められているセキュリティ要件の確認の代用とすることも考えられるため、小規模団体が調達する際の負担軽減に資するのではないかと思う。無論、どのような調達を行うかについては、最終的には自治体の判断になる。

○　クラウドサービスの選定について、地方公共団体の情報が外国のデータセンターに蓄積されている場合、「日本の法令の範囲内で運用できるデータセンターを選択する必要がある」との記載があるが、外国にデータセンターがある限り当該外国の法令が刑事訴訟については適用されるため、記載されている趣旨は成り立たないのではないのではないか。

●　政府統一基準群を参考に、ガイドライン改定案の修正を検討する。

以上