

# 令和4年 地方分権改革に関する提案募集 提案事項

総務省 最終的な調整結果

管理番号

289

提案区分

B 地方に対する規制緩和

提案分野

11\_その他

提案事項(事項名)

「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」における、マイナンバー利用事務系への接続にかかる規制緩和

提案団体

東京都

制度の所管・関係府省

総務省

求める措置の具体的内容

「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」における、マイナンバー利用事務系への接続にかかる規制を緩和し、テレワーク及び無線接続においても利用を可能とすること。

具体的な支障事例

【現在の制度】

「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」により、マイナンバー利用事務系のシステムに接続が許される環境は、各自治体庁内及び有線接続に限定され、テレワークにおける接続や無線接続は禁止となっている。

【支障事例】

税務職員が行う事務は税務情報を取り扱うものが大半であることから、マイナンバー利用事務系のシステムにアクセスするために、庁舎への出勤をせざるを得ず、全くテレワークを行うことができない。また、無線接続が禁止のため現地調査時にオンラインでの確認ができない。

例えば、現地調査中に土地の評価内容などを確認したい場合や、調査にて判明した事実、調査中に受け付けた納税者の申告について、システムに記録したい場合があったとしても、マイナンバー利用事務系内の税務情報システムに接続し、閲覧・記録することができないことから、帰庁後に調査結果をまとめて評価内容の確認や調査結果の記録、申告の反映をすることになり、事務効率及び納税者サービスがかなり劣る。

さらに、固定資産税(土地)評価事務では、1回の現地調査で多くの土地の利用状況などを確認するが、必要な情報は全て紙に打ち出して持ち出しており、ペーパーレスが実現できていない。

制度改正による効果（提案の実現による住民の利便性の向上・行政の効率化等）

税務システムの庁舎外での活用が可能になることにより、出張先における納税者からの問合せや追加で生じた調査事項に対し、庁舎に持ち帰っての確認や、再度の訪問をすることなく、きめ細かい対応が可能になり、納税者サービスの向上に資する。

また、現在は、出張で用いる調査票を紙で出力し、現地で記入した上で、帰庁後に税務システムに調査結果を入力する作業が生じているが、直接入力できることで二度手間が生じず、事務の効率化に資する。

根拠法令等

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

## 追加共同提案団体及び当該団体等から示された支障事例（主なもの）

宮城県、川崎市、富士見市、豊田市、長岡京市、兵庫県、佐世保市、宮崎県

○当市においてもテレワークを阻害する要因の1つに、マイナンバー利用事務系の業務担当課において、システムへの接続ができないことがある。マイナンバー利用事務系、特に税務システムにおいては住民対応せずに行う業務が多いため、効果が期待できる。

○将来的に事務のペーパーレス化や事務室のフリーアドレス化等による業務改善を検討しており、実現のためには全ネットワークの無線化が必要である。マイナンバー利用事務系の無線接続ができない場合、その関連部署では無線化できず、事務改善を実現できない。

○番号利用事務系ネットワークについて、閉域 LTE 網や WPA(Enterprise)等、高いセキュリティを確保した上で、各団体の判断により無線接続を行うことは問題ないとする。(想定しうる支障事例)臨時の執務室での書類審査等の対応を行う場合、有線 LAN の敷設等が必須となる。

## 各府省からの第1次回答

「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」は各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したものである。したがって、本ガイドラインで記述した構成や例文は、参考として示したものであり、各地方公共団体が独自の構成、表現により、情報セキュリティポリシーを定めることや、策定した情報セキュリティポリシーに基づき、独自のセキュリティ対策を行うことを妨げるものではない。

各地方公共団体が定める情報セキュリティポリシーに基づき、適切なセキュリティ対策を行っていただきたい。

## 各府省からの第1次回答を踏まえた提案団体からの見解

「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」の位置づけについては理解できるものの、本ガイドライン内で明確に不可と規定されていることにより、各自治体では無線LANの活用余地がないものと考えざるを得ず、各自治体の独自のセキュリティ対策が阻害されている。

本件について、各自治体の運用次第で活用余地があるのであれば、その旨を本ガイドライン内に明記いただくなど、各自治体が本ガイドラインの主旨を踏まえ、それぞれの状況に応じて適切にセキュリティ対策を検討・実施できるよう、ガイドラインの記載について、引き続き改善に向けたご検討をお願いしたい。

また、活用にあたっての技術的な要件など、セキュリティ対策における留意点があれば、ぜひご教示いただきたい。

## 各府省からの第1次回答を踏まえた追加共同提案団体からの見解

—

## 地方六団体からの意見

【全国知事会】  
提案団体の提案を考慮した検討を求める。

## 各府省からの第2次回答

「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(令和4年3月版)第1章本ガイドラインの目的等」において、「地方公共団体における情報セキュリティは、各地方公共団体が保有する情報資産を守るにあたって自ら責任を持って確保すべきものであり、情報セキュリティポリシーも各地方公共団体が組織の実態に応じて自主的に策定するものである。本ガイドラインは、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したものである。したがって、本ガイドラインで記述した構成や例文は、参考として示したものであり、各地方公共団体が独自の構成、表現により、情報セキュリティポリシーを定めることを妨げるものではない。」と記載しているところであり、本ガイドラインは各地方公共団体が独自の構成、表現により、情報セキュリティポリシーを定めることや、策定した情報セキュリティポリシーに基づき、独自のセキュリティ対策を行うことを妨げるものではない。各地方公共団体が定める情報セキュリティポリシーに基づき、適切なセキュリティ対策を行っていただきたい。

令和4年の地方からの提案等に関する対応方針（令和4年12月20日閣議決定）記載内容

—