地方税法施行規則第三条の三の二第三項、第五条の二第三項、第十条第五項、第十条の二の八第三項及び第二十四条の三十九第一項に規定する情報通信の技術の利用における安全性及び信頼性を確保するために必要な基準の一部を改正する告示（案）等に対して提出された意見及び総務省の考え方
（令和８年８月５日～９月８日）

「地方税法施行規則第三条の三の二第三項、第五条の二第三項、第十条第五項、第十条の二の八第三項及び第二十四条の三十九第一項に規定する情報通信の技術の利用における安全性及び信頼性を確保するために必要な基準の一部を改正する告示（案）等」に関して、令和８年８月５日（水）から令和８年９月８日（火）まで御意見を募集したところ、計 14 件の御意見をいただきました。

お寄せいただいた御意見とそれに対する考え方について、以下のとおり取りまとめましたので公表いたします。なお、取りまとめの都合上、御意見の内容を適宜整理しています。

No.	意見提出者	案に対する意見及びその理由	総務省の考え方	提出意見を踏まえた案の修正の有無
1	個人	■意見１：クラウド事業者選定における「原則」規定の例外要件及び手続の明確化 【該当箇所】 ・各告示案「機構委託クラウド事業者に係る事項」第１（機構委託クラウド事業者の選定） 【提案内容】 「機構は、原則として政府情報システムのためのセキュリティ評価制度のクラウドサービスリストに掲載されているクラウドサービスを提供することができる事業者を選定すること。」という規定に対し、以下の但し書きまたは注記を追加することを提案します。 「ただし、やむを得ない理由により同リストに掲載されていない事業者を選定する場合は、同等以上のセキュリティ水準を有することを事前検証し、その理由及び検証結果を記録するとともに、総務大臣に報告しなければならない。」 【理由】 現行案の「原則として」という表現のみでは、どのような場合に例外が認められるのか、また例外適用時にどのようなセキュリティ評価が必要とされるのかが不透明です。評価制度（ISMAP）未登録の事業者が十分な検証なしに選定されるリスクを防ぎ、透明性を確保するため、例外適用の要件と手続を告示上で明確に規定することが望まれます。この変更は文言の追記のみで可能であり、制度の信	意見１ 本基準案では、原則として ISMAP 等クラウドサービスリストからクラウドサービス事業者を選定することとされております。 例外的な取扱いについては、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及び地方公共団体における情報セキュリティポリシーを踏まえ、個別具体の状況に応じて判断されるべきものであるとされております。 意見２ 機構と機構委託クラウド事業者における責任分担について、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及び地方公共団体における情報セキュリティポリシーを踏まえ、ステークホルダーの役割と責任の範囲を把握して明確化することとされております。 意見３ インシデント発生時の報告について、各告	無

		頼性を著しく高めます。 ■意見２：機構と機構委託クラウド事業者における責任分界の明確化 【該当箇所】 ・各告示案「機構委託クラウド事業者との契約」第２ 【提案内容】 契約規定に以下の項目を明記することを提案します。 「機構は、クラウドサービスを調達する場合には、クラウドサービスモデルに応じた機構と機構委託クラウド事業者との責任分界（インフラ、プラットフォーム、アプリケーション、データ等の各階層における管理責任の区分）を調達仕様書及び契約において明確に定めなければならない。」 【理由】 告示案の各条項（体制整備や障害防止等）において「機構及び機構委託クラウド事業者は…行わなければならない」と双方に同等の義務を並列して課す規定が多く見られます。しかし、クラウド運用においては、インフラ管理とデータ・運用管理で責任主体が本質的に分かれます。障害発生時や事故発覚時に責任の所在が曖昧になることを防ぎ、迅速な初動対応を可能にするため、調達仕様及び契約において責任分界を明確に定めることを告示上で義務付けることが有効です。 ■意見３:インシデント発生時における事業者から機構への即時報告義務の明記 【該当箇所】 ・各告示案「緊急時体制」または「障害時等の対応」に関する規定 【提案内容】 障害発生時及びデータ漏えい等のセキュリティインシデント発生時における連絡体制規定において、以下の文言を追加することを提案します。 「機構委託クラウド事業者は、システムの障害、不正アクセス、データの漏えいその他これらに準ずる事態を検知した場合は、直ちに機構に報告し、被害拡大防止措置を講じなければならない。」 【理由】 現行案では、機構から総務大臣への報告義務（速やかに報告）は明確にされていますが、クラウド事業者から機構への報告義務やタイムラインに関する明確な記載が不十分です。クラウド環境におけるインシデントは初動対応の速さが被害規模に直結するため、事業者から機構への即時報告を義務付ける規定を追加することで、行政全体の対応力を大きく向上させることができます。 ■意見４：データレジデンシー及び国外からのリモート管理制限の明確化 【該当箇所】 ・各告示案「国税連携ネットワークシステムの環境及び設備」第３ 建物及び重要機能室	示案に規定される「機構の体制、規程等の整備」において、異常な状態を早期に発見するための監視体制、運用保守に関する規程及び操作手順書、緊急時対応計画並びに連絡体制の整備等を求めており、例外事案への対応に必要な基本的な枠組みを規定しています。 意見４ データ及び管理権限の取り扱いについて、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及び地方公共団体における情報セキュリティポリシーを踏まえ、アクセス制御機能の適切な運用を行うこととされております。 意見５ クラウド環境への移行について、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及び地方公共団体における情報セキュリティポリシーを踏まえ、情報システム更改時の対策について適切な措置を講ずることとされております。 いただいた御意見は、これらの運用を検討する際の参考とします。	

		・各告示案「機構委託クラウド事業者に係る事項」 【提案内容】 データ及び管理権限の取り扱いについて、以下の規定または注記を追加することを提案します。 「機構及び機構委託クラウド事業者は、地方税関係データ並びにシステム管理機能へのアクセスについて、原則として日本国内からのみ行われるよう必要な措置を講じなければならない。国外拠点からのリモート保守や運用を行う場合は、あらかじめそのリスクを評価し、適切な安全管理措置を調達仕様に含めること。」 【理由】 告示案では「建物等を国内に設置すること」と指定されていますが、クラウド運用においては、物理サーバーが日本国内にあっても、海外拠点からのリモートアクセスやバックアップ退避が行われるケースが存在します。データガバナンス及び外国法域の管轄リスク（情報開示請求等）への対応として、物理的な設置場所だけでなくアクセス・運用管理の所在についても明確化しておくことが重要です。 ■意見５：クラウド移行期（令和８年９月更改）における安全確保措置の追加 【該当箇所】 ・各告示案「その他」または附則 【提案内容】 移行期の取扱いとして、以下の事項を明確化することを提案します。 「令和８年９月24日の更改に伴うクラウド環境への移行にあたっては、データ移行時の暗号化、新旧環境の切替手順及び不測の事態における切り戻し（バックアウト）手順を定めた移行計画を作成し、安全性を確保した上で実施すること。」 【理由】 オンプレミスからクラウドへの全面移行は、システム運用上最もリスクが高まる局面の一つです。切替時のトラブルによる税務行政の停滞やデータ失念を防ぐため、移行計画の策定と安全確保を明記しておくことが、スムーズな移行と安心感の向上につながります。		
2	個人	1.事業者が「安全な器（インフラ）」を提供しても、機構や自治体側のシステム設定ミス（権限設定の間違い、API のセキュリティ不備など）があれば、容易にデータ漏洩が発生します。重大インシデント発生時に「どちらの責任か」の境界線が曖昧になり、初動対応が遅れるリスクがあります 2.：これほど巨大で機密性の高い税インフラを預けられるクラウド事業者は、市場で極めて限定的（外資系大手や国内のごく一部）になります。結果として特定の事業者に依存するベンダーロックインが発生し、将来的な利用料金の値上げに応じざるを得なくなったり、他社へのリプレイスが事実上不可能になった	御指摘いただいた責任分担、監視・監査、インシデント対応、ベンダーロックインへの懸念及び規定の手続き等について、自治体の負担にも配慮しつつ、これらの運用を検討する際の参考とします。	無

		りする硬直化を招きます。 3.機構側からシステムの深部が直接見えなくなるため（可視性の欠如）、内部で予兆なく発生しているサイバー攻撃や、クラウド事業者内部の人間による不正（内部不正）をタイムリーに見検知することが難しくなります。第三者認証や報告制度に依存せざるを得ない点が弱点です。 4.クラウド事業者側で大規模なネットワーク障害や設定ミス（数年に一度発生する世界規模のクラウドダウンなど）が発生した場合、全国の地方税の申告・電子納税、公金収納のすべてが同時に大停止します。分散管理されていた場合に比べ、インフラ障害時の社会的な影響範囲が爆発的に広がります。 5.「電子申告」「特定徴収金」「地方税関係通知」など、手続きごとに安全性・信頼性基準の告示がバラバラに分かれているため、全体としてのガバナンス（統制）が複雑化します。委託されるクラウド事業者側から見ても、複数の告示にまたがる基準を同時に満たし続ける必要があり、運用の形骸化や、基準の解釈ミスによるセキュリティホール（制度の隙間）が生じるリスクがあります 6.パブリックコメントが締め切られてから、わずか16日後（約2週間）にシステムが稼働し、新しい法的基準が施行されるスケジュールになっています。これでは、もし国民や民間企業、自治体から「この要件には重大なセキュリティリスクがある」と有益な指摘（意見）があったとしても、稼働までにシステムや告示案を修正・再検証する時間は物理的にありません。パブリックコメントが単なる「形式的な手続き」になっており、外部の意見を柔軟に取り入れて安全性を高める仕組みとして機能していない（スケジュール的な無理がある）点が大きな欠点です。 7.eLTAXの受け皿となる全国の地方自治体（市町村や都道府県）の現場への配慮が不十分です。足元の自治体では、令和8回（2026年）に向けて「地方公共団体情報システムの標準化（いわゆる自治体システム標準化）」の対応でただでさえ大混乱しています。このタイミングでeLTAX側の接続基準や安全基準の法的な枠組みが変わることは、自治体のIT現場に二重のシステム改修・運用の検証負担を強いることになり、現場の設定ミスによる障害を誘発するリスクが高まります AIを補助に問題点を出しましたが、上記全て解決できなければ問題だらけで失敗するでしょう		
3	個人	「セキュリティの為に」クラウド化、というのは、おかしいのではないか? ローカルサーバーであれば 外部からの侵入などに ある程度耐性が有るはずだが、営利目的の企業に データを預ける事に、危険性を感じる。 通信上の危険、企業からの流出の危険、企業による 悪意のある利用の危険など、各段に 個人情報への不安が増すはずだが、保障は出来るのか? 「政府が認可した企業だから信用」などというものではなく、物理的な保障を	クラウドサービスの利用のメリットとして、地方公共団体における情報セキュリティポリシーにおいて工数削減等に言及をされております。いただいたセキュリティの確保に係る御指摘について、各告示案や各告示案において示されている政府機関等のサイバ	無

		とるべきだ。 　また、ローカルサーバーであれば 単に その維持費だけで良いが、わざわざ外部の企業に 利用料を支払い続ける事も疑問だ。 　加えて、ネットワーク通信ありきでは、災害時などの対応が取れない可能性も高い。 　バックアップ強化を図りたいなら、単に 自治体間で 共有サーバーを設け、遠隔地に 複数のバックアップ（もちろん暗号化したもの）を作る方が、ずっと信頼性が高いのではないか。 　外部企業の技術を提供してもらうにしても、少なくとも、サーバーおよび内部データの所有は、行政内に置くべきだ。 　再検討を求める。	ーセキュリティ対策のための統一基準群及び地方公共団体における情報セキュリティポリシーを踏まえた安全な運用を行う際の参考とします。	
4	個人	今 ICC の赤根智子氏への、米国 トランプ政権による制裁が問題になっているが、そこでも、メールやクレジットカード、WEB サイトなど アメリカ企業の運営に依存するサービスの遮断が行われている。 　日本政府は 防衛省でアメリカのクラウド企業を利用する、などと 埒外な方針を発表しているが、税務となれば 国民の経済状況、国歌の歳入、交付金の振込口座など あらゆる情報が流出してしまう危険、また サービス遮断により行政が停止してしまう可能性がある。 　あくまでも クラウド利用の必要があるなら、国内企業による国内サーバーを用い、行政が権限と責任を持ち管理すべきである。	本基準案では、原則として ISMAP 等クラウドサービスリストからクラウドサービス事業者を選定することとされております。 　例外的な取扱いについては、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及び地方公共団体における情報セキュリティポリシーを踏まえ、個別具体の状況に応じて判断されるべきものであるとされております。	無
5	個人	本改正案において安全性及び信頼性の確保が謳われていること自体は否定しないが、近年の行政デジタル化の急速な推進、およびそれに伴う地政学的・構造的リスクの増大に照らし、現行の基準案およびその前提には看過できない重大な欠陥とリスクが存在するため、以下の通り再検討を強く求める。 　1. 個人情報の無断取得・目的外利用の防止と「同意」の形骸化の排除 　懸念点: デジタル化や共通化の推進に伴い、本人の予期しない形での個人情報の横断的収集や、実質的な同意の強制・形骸化が生じる危険性が極めて高い。 　法律やプライバシーポリシーの形式的遵守にとどまり、実質的な自己情報コントロール権が担保されない構造的リスクが放置されている。 　要望: データの保有・連携範囲に関する制限をより厳格化し、行政目的であっても本人に無断での二次利用や目的外突合が行われないための具体的な歯止めと監査基準を明記すること。 　2. 外資参入およびサプライチェーンを通じた情報流出・スパイリスクの遮断 　懸念点: コスト効率やグローバル調達の論理により、クラウドインフラ、システム開発、データ管理等のサプライチェーンに外資や地政学的リスクを抱える事業者が参入することの危険性が十分に認識されていない。	意見１ 　データ及び管理権限の取り扱いについて、各告示案において示されている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及び地方公共団体における情報セキュリティポリシーを踏まえ、アクセス制御機能の適切な運用を行うこととされております。 　意見２ 　本基準案では、「政府機関等の情報セキュリティ対策のための統一基準群」及び「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」を踏まえ、必要な措置を講じなければならないこととしており、情報システム・機器等の調達、再委託先を含む委託先事業者の選定等に際し、適切なサプライチェーン・リスク対策を講じること	無

		地方税務という国家の根幹をなす機微情報が、事実上の国外トランスファーや遠隔アクセスに曝されるリスクに対し、現在の安全性基準はあまりに形骸的かつ脆弱である。 要望: 重要インフラおよび機微データを扱うシステムへの外国資本の関与やオフショア開発・遠隔保守に対する法的・物理的な遮断要件を強化し、経済安全保障上のリスクを排する実効的な基準を追加すること。 3. 巨大集約化に伴う標的型攻撃リスクへの耐性評価 懸念点: システムの共通化・一元化は、国家主体や高度犯罪グループにとっての費用対効果を跳ね上げ、スパイ活動等、サプライチェーン全体を崩壊させるような致命的な情報流出の格好の標的を生む。 告示案が想定するような形式的なチェックリストの遵守では、高度化するサイバー脅威を防ぎきれない。 要望: 単なる基準への適合チェックではなく、侵入を前提としたゼロトラストアーキテクチャの強制や、万が一のインシデント発生時の被害極小化・トレーサビリティ確保に関する要件を抜本的に引き上げること。 4. 自治体現場の過重な疲弊とセキュリティガバナンスの形骸化の防止 懸念点: 度重なる国主導のシステム改修や複雑な基準対応、増大する監査負荷が、深刻な人員不足にあえぐ自治体現場にさらなる疲弊を強いている。現場のキャパシティを超えた形だけのデジタル化は、かえってセキュリティインシデントの予兆を見落とす「組織の盲目化」を招く。 要望: 基準の厳格化を図るのであれば、地方自治体の財政的・人的負担を直視し、国による十分な財政支援および専門的人材の直接派遣・技術支援をセットにした実効性のある仕組みに改めること。	を求めています。 意見３ インシデント発生時の報告について、各告示案に規定される「機構の体制、規程等の整備」において、異常な状態を早期に発見するための監視体制、運用保守に関する規程及び操作手順書、緊急時対応計画並びに連絡体制の整備等を求めており、例外事案への対応に必要な基本的な枠組みを規定しています。 意見４ 御指摘いただいた自治体の負担について、今後の運用を検討する際の参考とします。	
6		今回の改正により、eLTAX の更改に伴って、これまで地方税共同機構がオンプレミスで管理していたサーバを、機構が委託するクラウド事業者が管理することとなり、ISMAP クラウドサービスリスト掲載サービスを原則として選定するとともに、選定基準を調達仕様に含め、契約に反映することとされています。この方向性に賛同します。 一方、クラウド事業者の選定、アクセス制御、監視、バックアップ、不正アクセス対策等を適切に実施しても、認証情報の窃取、設定不備、未知の脆弱性、内部不正、委託先・再委託先の侵害等を完全に防止することは困難です。 国家サイバー統括室の重要インフラに関する基準でも、あらゆるサイバー攻撃から完全に防御することは困難であり、障害等が発生した場合の影響を許容範囲内に抑えるレジリエンスの確保が必要との考え方が示されています。 eLTAX は、地方税の申告、納税その他の重要な情報を全国規模で取り扱う基盤	インシデント発生時の報告について、各告示案に規定される「機構の体制、規程等の整備」において、異常な状態を早期に発見するための監視体制、運用保守に関する規程及び操作手順書、緊急時対応計画並びに連絡体制の整備等を求めており、例外事案への対応に必要な基本的な枠組みを規定しています。いただいた御意見は、これらの運用を検討する際の参考とします。	無

		です。 クラウド移行を機に、「侵入を防ぐ」対策だけでなく、「侵入や情報流出が発生した場合にも、流出したデータそのものから生じる被害を最小化する」という観点を、機構委託クラウド事業者の選定基準、調達仕様及び契約に明確に位置付けることを提案します。 具体的には、リスクに応じて以下の事項を技術中立的な性能要件として検討していただきたいと考えます。 ① 単一のクラウド環境、管理アカウント、端末又は委託先・再委託先が侵害された場合にも、取得されたデータ単体では原情報の復元・悪用が困難であること。 ② 保存データ、バックアップ、移行時の一時データ等について、暗号化に加え、秘密分散、データ無意味化、分散保管、暗号鍵とデータの分離等を含む多層的なデータ保護を選択できること。 ③ 職員が個々の情報について保護の要否や保存方法を都度判断しなくても、通常の業務フローの中でシステム側が必要な保護を自動的に適用できること。 ④ 再委託を含む委託の連鎖においても、同等のデータ保護要件が維持されること。 特に③については、セキュリティを利用者個人の判断や注意だけに依存させず、通常どおり業務を行うことで必要な保護が適用される仕組みとすることが、誤操作や設定ミス等による漏えいリスクの低減にもつながると考えます。 また、秘密分散技術については、経済産業省のサプライチェーン強化に向けたセキュリティ対策評価制度に関する意見募集結果においても、「セキュリティ侵害に対する被害の最小化に有効な手段の一つ」との認識が示されています。 特定企業又は特定製品の採用を求める趣旨ではありません。 ISMAP 等によるクラウドサービス自体の安全性確保に加えて、「流出したデータ単体では復元・悪用が困難である」「単一の侵害点から原データ全体を取得できない」といった、データ自体の耐侵害性についても性能要件として評価することを要望します。 以上、よろしくお願いいたします。		
7	個人	取り扱い情報の安全性のため、行政及び申告者の端末や情報機器には中国製使用を禁じる。また、掛かる請負業務も中国系企業の参加を禁じる。	本基準案では、「政府機関等の情報セキュリティ対策のための統一基準群」及び「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」を踏まえ、必要な措置を講じなければならないこととしており、情報システム・機器等の調達、再委託先を含む委託先事業者の選定等に際し、適切なサプライチェーン・リスク対策を講じること	無

			を求めています。	
8	個人	リージョンの指定についての情報が見当たらなかったが、そういうのは指定するとはしないのであろうか？ クラウド事業者のクラウド上で運営されるホストのサーバは香港のものであったりする事もそれなりに多いのであるが（金融庁や国税庁の、国民の意見を受け付けるようなサーバがそのようなクラウドで運用されるサーバで提供されていたりもする（そしてデータの送信先が香港やシンガポールになっていたりする。）。もちろん肯定的には見れない。金のまともな使い方を分かっていない、ICT時代に適切に対応していない、質の低い者達だとも見る。）、香港は中国に属する区域となっているのであり、日本国の機関が運用するサービスがそういうホスト（※加えて、日本から発信された情報が中国宛に通信される事もであろうか。なお途中の通信路や海底光ファイバー事業者などについても疑うべき部分がある事を述べておく。）から提供される事は、当然事態として容認できるものではない。回避策としては、クラウドの使用リージョンについて国内のものを使用する事がとりあえず有用なものとして挙げられるはずであるが（クラウド事業者においてのバックアップデータ等も国内他ホストに保有されるようなものが適切ではないかと思われる。）、国は、日本国の機関（地方公共団体も含めた方が良いのではないかと思われるが）が、クラウド事業者のクラウドサービスを利用する場合、特段に在他国のホストを使用する必要性がある場合以外は、国内リージョンでのサービス提供が行われるコース・プランに利用を制限すべきではないかと考える。 他文書においてそのような制限についての記述があるのかもしれないが、もしもそのような制限が存在しないのであればそれは良くないと思われるので、そのような制限があるようにされたい。	本基準案では、「政府機関等の情報セキュリティ対策のための統一基準群」及び「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」を踏まえ、必要な措置を講じなければならないこととしており、情報システム・機器等の調達、再委託先を含む委託先事業者の選定等に際し、適切なサプライチェーン・リスク対策を講じることを求めています。なお、主要な情報システムの所在地についても、国内設置を求めることとしています。	無

9	個人	総務省「地方税法施行規則における情報通信技術の安全性・信頼性基準の一部改正案」について、以下のとおり意見を提出いたします。 今回の告示案は、地方税のオンライン手続きに関する情報通信技術の安全性・信頼性基準を、最新の技術環境に合わせて見直すものと理解しております。しかし、資料には成果目標やKPI（重要業績評価指標）が存在せず、制度改正の効果を客観的に検証するための仕組みが不足していると考えます。地方税のオンライン手続きは国民の最重要個人情報を扱うため、制度の透明性と実効性を確保するためには、必ずKPIを設定し、継続的に監視する必要があります。 ―――――――――――――――――――― 【1．本案件に必須と思われるKPIの例】 （1）自治体の基準適合率 理由：改正後、どれだけの自治体が新基準に適合できたかを測れます。 （2）情報漏えい件数（改正前後の比較） 理由：安全性向上の効果を直接測定できます。 （3）不正アクセス検知件数 理由：新基準が実際に脅威を減らしているか確認できます。 （4）セキュリティ事故対応時間（平均） 理由：自治体の対応力向上を測る指標です。 （5）電子申請システムの障害発生率 理由：基準改正がシステム安定性に寄与しているか確認できます。 ―――――――――――――――――――― 【2．KPI算出のためのデータを誰がどこから集めるべきか】 ●総務省（自治行政局・情報セキュリティ室） ・自治体の基準適合状況 ・セキュリティ事故報告 ・電子申請システムの障害情報 ●自治体（都道府県・市区町村） ・情報漏えい件数 ・不正アクセス検知ログ ・事故対応時間 ●デジタル庁 ・自治体DXの進捗 ・マイナポータル連携状況 ・電子申請基盤の利用統計 ●内閣官房（サイバーセキュリティセンター） ・全国的なサイバー攻撃の傾向 ・自治体への攻撃情報	本基準案は、地方税法にeLTAXを通じて申告等、特定徴収金の収納、地方税関係通知を行う規定があるものについて、情報の取扱い等を定めるものであり、成果目標・KPI等の性質に馴染まないことから、本基準案の修正は行いません。いただいた内容は御意見として承ります。	無

		これらを統合して制度の効果を客観的に検証する必要があります。 ―――――――――――――――――――――――― 【3. 行政手続法 39 条 2 項との整合性】 行政手続法 39 条 2 項は、「公示する命令等の案は、具体的かつ明確な内容であり、題名および根拠条項が明示されていること」を求めています。 しかし今回の告示案は、 ・成果目標 ・検証方法 ・達成期限 が具体的に示されておらず、行政手続法 39 条 2 項の趣旨に照らして不十分です。 行政官の皆様には、納税者の信頼を損なわないためにも、法令の趣旨を丁寧に理解し、透明性の高い制度設計を行っていただきたく存じます。もし、こうした基本的な要件を満たすことが難しい場合は、ご自身の適性を静かに振り返り、納税者にとって害にならない選択を考えていただくことも必要ではないかと感じます。 ―――――――――――――――――――――――― 【4. 高市政権の「縦割り行政の壁を超える方針」との整合性】 高市政権は「外国人政策・社会保障・エネルギー・AI など戦略分野で縦割り行政の壁を超えて連携する」ことを閣僚に指示しています。 しかし今回の告示案は、 ・総務省単独で完結しており、 ・デジタル庁（自治体 DX） ・内閣官房（サイバーセキュリティ） ・財務省（税務システム連携） との連携の記述がありません。 地方税のオンライン手続きは複数省庁が関わる領域であるため、 高市政権の方針（縦割り行政の打破）に反している可能性が高いです。 ―――――――――――――――――――――――― 【5. AI・AX・DX との協調】 地方税のオンライン手続きは、 ・電子申請 ・データ標準化 ・AI による不正アクセス検知 など、DX と非常に相性が良い領域です。 しかし今回の告示案には、 ・デジタル庁との協調		

		・DX 推進の記述 がありません。 DX の観点から制度設計が不十分である可能性があります。 ―――――――――――――――――――――――――――― 【6. 他部署との連携が書かれていない点について】 本来連携すべき部署は以下のとおりです。 ・デジタル庁（電子申請・自治体 DX） ・内閣官房（サイバーセキュリティ） ・財務省（税務システム連携） ・総務省統計局（データ品質管理） 今後のパブコメ案件では、 「どの省庁と連携し、どのデータを共有するのか」 を必ず明記するよう促します。 ―――――――――――――――――――――――――――― 【7. 成果目標・KPI が存在しない場合に求める事項（EBPM の観点）】 政府は既に全府省庁・原則全事業を対象として EBPM および行政事業レビューを実施しています。その趣旨に照らし、本案件について成果目標および客観的な効果検証指標が設定されていない理由を明示してください。 併せて、 ・成果指標 ・基準値 ・目標値 ・達成期限 ・予算との連動状況 を設定し、公表してください。 KPI は多ければ良いわけではなく、記録項目が増えるほど誤記載や見逃しが増えます。最小限の時間とコストで最大の効果を得られるよう、バランスを考えて制度設計していただくことを強くお願い申し上げます。 「客観的な成果目標と KPI」の設定と運用によって、少なからず人命や生活を守る機会も生まれます。スペーシア事故のように、作業への慣れから緊張感が薄れ、確認不足や手順省略による事故が増える傾向は多くの現場で指摘されています。KPI という数値データの増減で危険性に気づく機会を作ることができます。 また、最初から完璧な KPI を作る必要はありません。まずは 50%程度の完成度を目安に設定し、2 か月～半年間隔で見直す運用を提案いたします。 ――――――――――――――――――――――――――――		
10	個人	「第 6 機構委託クラウド事業者に係る事項」の「1 機構委託クラウド事業者	本基準案では、原則として ISMAP 等クラウ	無

		の選定」において、 「機構は、原則として政府情報システムのためのセキュリティ評価制度のクラウドサービスリストに掲載されているクラウドサービスを提供することができる事業者を選定すること。」とされています。 しかし、「原則として」と規定する以上、ISMAP クラウドサービスリストに掲載されていないクラウドサービスを提供する事業者を選定する例外が想定されますが、その例外を認める条件や判断基準が本告示案からは明らかではありません。 地方税に関する情報は、多数の地方公共団体及び納税者に関係する重要な情報であり、その電子申告等受付システムについては特に高い安全性及び信頼性の確保が求められると考えます。 このため、ISMAP クラウドサービスリストに掲載されていない事業者を例外的に選定することを認めるのであれば、どのような場合に例外を認めるのか、また、その場合にどのような方法により ISMAP と同等以上の安全性及び信頼性を確認するのかについて、明確な基準を示すべきではないでしょうか。 「原則として」という規定のみでは例外適用の判断に一定の裁量が生じ得るため、地方税情報を取り扱うシステムの安全性及び信頼性を確保する観点から、例外を認める場合の要件又は判断基準を明確化することを要望します。	ドサービスリストからクラウドサービス事業者を選定することとされております。 例外的な取扱いについては、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及び地方公共団体における情報セキュリティポリシーを踏まえ、個別具体の状況に応じて判断されるべきものであるとされております。	
11		今回の改正は、これまでオンプレミスで管理されていた eLTAX のサーバを民間クラウド事業者が管理する方式へ移行することに伴うものであり、地方税に関する重要な情報の管理形態を変更する重要な制度改正と考える。 しかし、説明資料では制度改正の必要性は示されているものの、従来のオンプレミス方式とクラウド方式について、安全性、信頼性、障害発生時のリスク、情報漏えいリスク等をどのように比較・検証したのかが明らかではない。 特に、クラウド事業者への委託に加え再委託も想定されていることから、情報管理に関与する事業者が増加することによるリスク及び責任の所在について、十分な説明が必要ではないか。 また、クラウド事業者について一定のセキュリティ基準を満たす事業者を「原則として」選定するとしているが、「原則として」とした以上、例外的な選定も想定される。「原則」の例外を認める具体的条件及び、その場合の安全性・信頼性をどのように担保するのか明らかにされたい。 単にクラウド化に対応するため基準を改正するだけでなく、従来方式と比較して安全性及び信頼性がどのように確保・向上するのか、具体的な比較・検証結果を国民及び地方公共団体に示すべきではないか。	再委託については、本基準案において、機構の事前承認を必要とし、再委託先に同等のセキュリティ対策を実施させること、再委託の条件、責任、報告及び監査等の安全性を確保するために必要な事項を契約に定めることを既に規定しています。また、事業者選定については、例外的な取扱いについては、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及び地方公共団体における情報セキュリティポリシーを踏まえ、個別具体の状況に応じて判断されるべきものであるとされております。	無
12		本案は、eLTAX のサーバーを地方税共同機構によるオンプレミス管理から委託クラウド事業者の管理へ移すことに伴い、既存の安全管理義務の実施主体に同事業者を追加するものです。クラウド事業者にも安全管理義務を負わせること	意見１ 本基準案では、原則として ISMAP 等クラウドサービスリストからクラウドサービス事	無

		自体は必要です。しかし、国民が提出を拒めない税務情報を再委託先を含む民間事業者に管理させる制度として、次の点が不明確です。 1　各案で ISMAP 登録サービスの利用を「原則として」としているため、未登録サービスを選べる余地があります。例外を認める要件、承認者、リスク評価、記録及び公表を告示上明記してください。要件を定められないなら「原則として」を削除し、登録サービスの利用を必須とすべきです。 2　「機構委託クラウド事業者」の定義には再委託先も含まれます。一方、新設される事業者選定規定が全ての再委託先に個別に適用されるのか明瞭ではありません。再委託の段階を制限し、全ての再委託先について機構の事前審査及び承認、国内設置、同等の安全管理、監査受入れ、責任分担を明記してください。 3　選定基準、委託先及び税務情報を扱う再委託先、役割分担、監査結果、事故時の対応状況について、セキュリティを害しない範囲で公表してください。漏えい等の際には総務大臣への報告だけでなく、関係地方公共団体及び影響を受ける本人への通知主体と期限も明確にすべきです。 4　意見募集の締切は 9 月 8 日、施行及び eLTAX 更改は 9 月 24 日とされ、間隔は 16 日しかありません。意見を検討し、告示、契約及び運用へ実質的に反映できる日程なのか説明してください。意見募集結果と最終告示は移行前に公表し、重要な修正を反映できない場合は施行を延期して再度意見を募集すべきです。 安全措置を非公開の調達仕様や契約だけに委ねず、例外、再委託及び責任の範囲を国民が確認できる告示にしてください。	業者を選定することとされております。 例外的な取扱いについては、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及び地方公共団体における情報セキュリティポリシーを踏まえ、個別具体の状況に応じて判断されるべきものであるとされております。 意見２ 再委託については、本基準案において、機構の事前承認を必要とし、再委託先に同等のセキュリティ対策を実施させること、再委託の条件、責任、報告及び監査等の安全性を確保するために必要な事項を契約に定めることを既に規定しています。 意見３ 個別の契約の詳細については、セキュリティリスクの観点から具体的なお答えは差し控えさせていただきますが、政府統一基準群等及び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を踏まえ、地方税共同機構において必要な体制の整備を図っております。 意見４ eLTAX の更改に向けたスケジュールについてのご意見は、関係機関の負担にも配慮しつつ、これらの運用を検討する際の参考とします。	
13		本告示案等の公表および意見募集にあたり、現在日本社会を深刻に蝕む経済格差の拡大というすべての元凶、および行政手続きのデジタル化推進に伴う生活者への不利益に対する重大な懸念から、以下の通り強く意見を述べさせていただきます。 第一に、地方税等のオンライン申請や情報通信技術の利用基準改定にあたり、行政側の効率化やシステム導入ばかりを優先し、デジタル機器に不慣れな高齢者や通信環境を持たない住民を置き去りにする運用は断じて容認できません。納税や行政サービスは全ての国民に課された義務であり権利であって、特定のデジタル手段を事実上強要・優遇するような差別的取扱いは制度の根幹を揺るがすものです。	本基準案に対する具体的な反対の理由は明らかではありませんが、地方税法に eLTAX を通じて申告等、特定徴収金の収納、地方税関係通知を行う規定があるものに関する情報の取扱い等を定めるものです。いただいた内容は御意見として承ります。	無

		第二に、総務省および自治体が最優先で果たすべきは、過度なデジタル偏重による「デジタル難民」の発生防止であり、紙の書類や対面窓口といった物理的な手続き手段を確実に残すことです。形骸化した効率化ごっこを排し、あらゆる生活環境にある住民が等しく不当な負担なく手続きを行える公正な行政基盤の維持を強く求めます。		
14		税務署 OB の税理士試験免除制度に関する改革および癒着防止策の強化についての意見 1. 意見の要旨 長年税務署職員として勤務したことによる税理士試験の一部免除制度については、現在の税務行政の公平性と、税理士業界全体の信頼性を著しく損なう懸念がある。特に、「元税務署職員」という肩書きを「税務署への影響力」として広告し、集客を行う税理士の存在は看過できない。電子化による安全性の確保のみならず、長年慣習化しているこのような制度および体制の抜本的な改善と見直しを強く求める。 2. 問題の背景と実態 税理士試験を正当なプロセスで突破した税理士にとって、元税務署職員であるという理由だけで税理士資格を得た者が、その特権的な立場を利用して不適切な営業活動を行うことは、公平な競争環境を阻害する要因となっている。 さらに深刻な問題として、税務署との「癒着」を想起させる事案が後を絶たないことが挙げられる。 3. 具体的事例（不正の疑いがあるケース） 確定申告を怠っていた経営者が税務調査の通知を受け、慌てて元税務署職員の税理士に依頼した事案がある。この際、当該税理士が「今後は私が責任を持つ」と税務署側へ介入した結果、本来科されるべき重加算税が免除され、極めて少額の追徴課税のみで決着したというケースを聞いた。 このような事態は、一般納税者から見れば「税理士が税務署と結託して脱税を見逃している」「元職員であれば税務調査で便宜が図られる」という不信感を抱かせるに十分な事案であり、税務行政全体に対する国民の信頼を根底から揺るがすものである。 4. 改善提案 電子記録や取引の安全性・信頼性を確保する制度構築は重要であるが、それと同等以上に、以下の体制改善に注力すべきである。 ・税理士試験免除制度の見直し： 公務員としての職務経験と、税務知識の専門性は必ずしもイコールではない。現行の免除制度を廃止、あるいは厳格化し、一般の税理士と同様の試験通過を必須とすべきである。 ・税務署 OB に対する倫理規定と監視の強化： 税務署 OB が特定の案件において、過去の勤務先に対して不当な働きかけを行うことを厳格に制限し、違反した	本基準案に対する具体的な反対の理由は明らかではありませんが、地方税法に eLTAX を通じて申告等、特定徴収金の収納、地方税関係通知を行う規定があるものに関する情報の取扱い等を定めるものです。いただいた内容は御意見として承ります。	無

		場合には厳しいペナルティを課す枠組みが必要である。 ・「影響力」を謳う営業活動の規制：「税務署に口が利ける」といった、公平性を疑わせるような誇大広告や勧誘行為に対する取り締まりを強化すべきである。 税務行政の公平性と透明性を確保するため、長年の慣習にとらわれず、国民が納得できる制度設計への改革を切に求める。		

【提出意見　14 件】