「地方税共同機構による地方公金の収納事務に係る安全性及び信頼性の確保に必要な基準（案）」に対して提出された御意見及びそれに対する総務省の考え方
（意見募集期間：令和8年7月23日（木）から同年8月26日（水）まで）

別紙

No.	意見提出者	案に対する御意見及びその理由	御意見に対する考え方	基準への反映の有無
1	個人A	【提出にあたっての基本方針】 本意見は、告示案で定められた安全性および信頼性の確保措置の趣旨に賛同しつつ、制度の実効性・運用の現実性・利用者の利便性をさらに高める観点から、文言の修正・追記等によって比較的容易に反映可能な改善項目を整理・提案するものです。 ---------- 【意見1】 該当箇所: 別紙1「特定歳入等及び特定歳入等に関する情報の取扱い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（案）」 第7 機構委託クラウド事業者に係る事項 1 機構委託クラウド事業者の選定（13ページ） 意見の要旨: クラウドサービスの選定において「原則として」例外を認める場合の評価・明確化プロセスの規定を追加すること。 該当箇所の本文（案）: 「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。」 修正案: 「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。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、選定理由および代替のセキュリティ評価結果を明確にし、文書により記録・保存すること。」 提案理由: 現在の案では「原則として」とされており、例外規定の適用条件や評価基準が明確ではありません。例外的な選定が認められる条件と、その際の客観的なセキュリティ評価記録の保存義務を明確化することで、運用の透明性を確保し、外部監査時の根拠としても機能するため、制度の実効性が大きく向上します。また、大きな制度変更を伴わずに文言の追記のみで対応可能です。 ---------- 【意見2】 該当箇所: 別紙1「特定歳入等及び特定歳入等に関する情報の取扱い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（案）」 第3 体制、規程等の整備 4 緊急時体制 （2）および（3）（4から5ページ） 意見の要旨: 大規模な障害発生時や情報漏えい時における「利用者（納付者）への周知・情報共有」に関する規定を追加すること。 修正案（第3の4（2）ウとして追加）: 「ウ 支払情報等の漏えいその他これに準ずる重大な事態が発生し、利用者に影響が及ぶおそれがある場合は、速やかに適切な方法により利用者に通知または公表を行うとともに、問合せ対応体制を整備すること。」 提案理由: 現行案では、障害や漏えい発生時の総務大臣への報告や連絡体制、復旧計画（第3の4（3））は盛り込まれていますが、実際に納付を行う利用者（国民・事業者）に対する情報共有の手続きが明確ではありません。特に電子納付においては、納付トラブルや個人情報に関する不安を迅速に解消することが信頼確保のために不可欠です。既存の「個人情報の保護に関する法律」や政府ガイドラインの趣旨と整合させる形での規定追加は容易であり、行政サービスの信頼性を一層高めます。 ---------- 【意見3】 該当箇所: 別紙1「特定歳入等及び特定歳入等に関する情報の取扱い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（案）」 第5 機構における運用管理上の安全性及び信頼性の確保 4 運用保守端末機及び払込端末機の管理 （1）ア（8から9ページ） 意見の要旨: 運用保守端末等の操作に関する「複数人対応」について、緊急時の例外措置および事後検証に関する追記を行うこと。 該当箇所の本文（案）: 「また、操作者による不正な行為及び誤操作による障害発生を防止するため、運用保守端末機及び払込端末機を操作する際は複数の者で行うこととすることなど、必要な措置を講ずること。」 修正案: 「また、操作者による不正な行為及び誤操作による障害発生を防止するため、運用保守端末機及び払込端末機を操作する際は原則として複数の者で行うこととすることなど、必要な措置を講ずること。ただし、夜間・休日等の緊急対応において複数人の配置が困難な場合であっては、操作ログの厳重な記録および事前許可・事後承認の手続きを講じることで代えることができる。」 提案理由: 複数人での操作原則はセキュリティ上極めて重要ですが、夜間・休日の緊急障害対応時など、現場の人的リソースが限られる状況において原則を厳密に適用しすぎると、かえって障害復旧の遅れを招くリスクがあります。セキュリティレベルを落とさずに代替手段（ログ記録・事前事後承認）を認める柔軟性を明記することで、実際の運用現場での実効性が著しく向上します。 ---------- 【意見4】 該当箇所: 別紙1「特定歳入等及び特定歳入等に関する情報の取扱い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（案）」 第5 機構における運用管理上の安全性及び信頼性の確保 3 地方税共通納税システムの運用保守等 （5） 無害化処理の実施（8ページ） 意見の要旨: 「無害化処理」の具体的な定義・手法について、将来の技術動向やデータ多様化に対応できる柔軟な記述とすること。 該当箇所の本文（案）: 「無害化処理（インターネット回線を経由して送信された支払情報発行依頼情報及び納付情報をテキスト形式に変換する方法等により不正プログラムが混入しないよう安全を確保する措置をいう。）」 修正案: 「無害化処理（インターネット回線を経由して送信された支払情報発行依頼情報及び納付情報をテキスト形式に変換する方法その他の技術的に適正と認められる方法により不正プログラムが混入しないよう安全を確保する措置をいう。）」 提案理由: 現在の定義例では「テキスト形式に変換する方法等」とありますが、技術の進歩に伴い、サニタイジングや最新の高度無害化技術など、より効率的な手法が登場する可能性があります。例示として「その他の技術的に適正と認められる方法」を加えることで、将来のシステム拡張やセキュリティ技術のアップデート時に基準の改定を要さず柔軟に対応できるようになります。 ----------	【意見1】 本基準案では、原則としてISMAPクラウドサービスリスト又はISMAP-LIU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個別具体の状況に応じて判断されるべきものであることから、一律の例外規定は設けませんが、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。 【意見2】 大規模な障害発生時や情報漏えい時に限らずシステムエラーが生じた場合には情報共有等の対応が必要になるところ、事象に応じて個別具体の判断が必要となることから、本基準案の修正は行いませんが、いただいた御意見は、制度運用の参考とさせていただきます。 【意見3】 本基準案では、操作者による不正な行為及び誤操作を防止するために必要な措置を求めるものであり、「複数の者で行うこととすることなど」としていることから、複数人による操作以外にも適切な代替措置を講ずることも可能であり、状況に応じた「適切な措置」を講じることが出来るよう規定しています。 よって本基準案の修正は行いませんが、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。 【意見4】 本基準案では、「テキスト形式に変換する方法等」と規定しており、「等」には、テキスト形式への変換以外の方法であって、不正プログラムが混入しないよう安全を確保できるものも含まれます。 したがって、将来の技術進展に応じた適切な無害化手法を採用することは現行案においても可能であることから、本基準案の修正は行いませんが、いただいた御意見は今後の運用を検討する際の参考とします。 【意見5】 今後の対応の参考とさせていただきます。	無

No.	意見提出者	案に対する御意見及びその理由	御意見に対する考え方	基準への反映の有無
		【意見5】 該当箇所: 別紙3「意見募集要領」 4 意見の提出方法・提出先 (2) 電子メールを利用する場合(1ページ) 意見の要旨: 電子メールによる意見提出時の受入れファイル形式に「PDFファイル」を追加すること。 該当箇所の本文(案): 「添付ファイルを送付する場合、ファイル形式は、テキストファイル、マイクロソフト社 Word ファイル、ジャストシステム社一太郎ファイルにより提出してください」 修正案: 「添付ファイルを送付する場合、ファイル形式は、テキストファイル、PDFファイル、マイクロソフト社 Word ファイル、ジャストシステム社一太郎ファイルにより提出してください」 提案理由: 官民問わず、文書の送受信における標準的なフォーマットとしてPDFが極めて広く普及しています。行政手続きのデジタル化や利用者の利便性向上の観点から、受入れ可能ファイル形式にPDFを追加することは運用の見直しのみで即時に実施可能であり、パブリックコメント提出者の負担軽減および多様な意見収集に大きく寄与します。 ---------- 【まとめ】 以上の提案は、いずれも提示されたセキュリティ水準や基本方針を維持しつつ、実際の運用現場での確実な実行、障害発生時の利用者保護、および将来の技術革新への適用性を補強するものです。貴省における最終決定の際、前示の修正案のご採用につきご検討いただけますと幸いです。		
2	個人B	【意見1】 該当箇所 第5の運用管理・障害対応・共通口座の管理、第6の他システムとの接続に関する規定 意見 誤納付、二重納付、納付済みであるにもかかわらず未納として表示される事案、収納情報の反映遅延その他の例外事案について、検知、照合、訂正及び納付者への案内の手順を明確化されたい。 また、地方税共同機構、地方公共団体、決済関係事業者及び委託先の間で、例外事案を共通して取り扱うための受付・連携様式を整備されたい。様式には、少なくとも案件識別番号、受付日時、対象公金、現在の処理主体、処理状況、照会先、次に行う対応、次回回答予定日及び納付者への案内内容を含めることが望ましい。 機構側又は関係事業者側で照合中の事案については、その状況を地方公共団体へ確実に連携し、地方公共団体が法令及び条例に沿って督促その他の不利益取扱いを適切に判断できる運用も明確化されたい。 理由 地方公金の収納において納付者の不安や負担に直結するのは、支払ったにもかかわらず未納となる、二重に支払ってしまう、又は問い合わせ先が分からないといった事案である。安全性及び信頼性には、不正侵入等を防止することだけでなく、収納情報の不整合を正確かつ速やかに訂正し、関係者間でたらい回しを生じさせないことも含まれる。 例外事案の情報項目と引継ぎ方法をあらかじめ標準化すれば、自治体規模や委託関係の違いによる運用差を抑え、納付者への説明と訂正を迅速化できる。 【意見2】 該当箇所 第3の体制整備・緊急時対応、第5の情報管理・障害対応・委託管理・自己点検及び外部監査、第6及び第7の外部接続・クラウド利用に関する規定 意見 収納処理の停止、不正アクセス、情報漏えい、誤収納、連携不全その他、納付状況、個人情報、納期限又は不利益取扱いに影響を及ぼすおそれのある事案が生じた場合について、地方税共同機構、地方公共団体、決済関係事業者、委託先及び再委託先の間における確認主体、納付者への説明主体、訂正主体及び再発防止措置の担当をあらかじめ明確化されたい。 影響を受けるおそれのある納付者への通知又は案内に当たっては、障害の発生事実だけでなく、納付が有効に処理されているか、再度納付すべきか、未納扱いとなる可能性があるか、次にどこへ問い合わせるべきかを判断できる内容とされたい。 また、外部監査については、地方公共団体が住民への説明責任を果たせるよう、自らの収納事務に関係する範囲で、監査の実施状況、主要な指摘及び改善状況を確認できる仕組みを整備されたい。ただし、具体的な脆弱性情報等、かえって安全を損なう情報の共有は慎重に取り扱うことが適当である。 理由 共同収納では関係者が多いため、問題発生時に責任や問い合わせ先が分散しやすい。内部的な役割分担だけでは、納付者にとって「自分の納付はどうなっているのか」「誰に相談すればよいのか」が分からない状態を防げない。 また、地方公共団体は住民に対する説明責任を負うことから、機構又は委託先における監査・改善の状況について、必要な範囲で把握できることが信頼性の確保に資する。 【意見3】 該当箇所 第2の利用者による送受信、第3の問合せ対応及び運用体制に関する規定 意見 高齢者その他、デジタル手続又は説明文の理解に負担を感じる納付者に対し、平易な表現による案内、画面操作の補助及び適切な相談先への案内を整備されたい。 その補助手段の一つとして、AIを用いた手順説明又は問合せの振り分けを活用することは有用と考えられる。ただし、AIは個別の納付状況、減免の可否、法的判断その他の重要な判断を自動的に行うものではなく、一般的な手順説明及び相談先案内を補助する範囲に限定されたい。 あわせて、電話、対面、紙媒体その他の手段を、AI利用が困難な場合の単なる代替ではなく、同等に利用可能な正式な相談経路として確保されたい。AIによる案内が誤り又は不十分であった場合にも、納付者が不利益を受けず、有人窓口で確認・訂正できる経路を明確化されたい。 理由 制度が技術的に安全であっても、納付者が操作方法、納付状況又は次に取るべき行動を理解できなければ、誤納付、未納不安及び問い合わせの集中を招く。特に、公金の納付は生活上の負担や不利益に結び付き得るため、理解しにくさを納付者の自己責任として残さない設計が必要である。 AIは、分かりやすい説明や窓口案内の補助として有用である一方、誤案内、利用困難者、個人情報の過剰入力といったリスクもある。したがって、AI導入そのものではなく、有人支援へ確実に戻れることを含めた利用者支援の仕組みとして整備することが、安全性及び信頼性の向上につながる。	【意見1】 本基準案では、「第3 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。 以上を踏まえ本基準案の修正は行いませんが、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。 【意見2】 本基準案では、地方税共同機構における特定歳入等に関する情報の取扱い等を定めるものであり、関係者の責任・連絡体制等や、異常時の対応及び監査等について必要な枠組みを定めています。事案に応じた役割分担、利用者への案内及び監査結果の取扱いについては、情報セキュリティ上の配慮を含め、「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に関するガイドライン」を踏まえて必要な措置を講じることを求めています。従って、本基準案の修正は行いませんが、御意見は今後の運用の参考とします。 【意見3】 本基準案では、「第3 機構の体制、規程等の整備」において、利用者支援及び誤操作防止のための問合せ窓口の設置を求めています。 具体的な方策は、運用において適切に検討されるべき事項であるため、本基準案の修正は行いませんが、いただいた御意見は、今後の運用を検討する際の参考とします。	無

No.	意見提出者	案に対する御意見及びその理由	御意見に対する考え方	基準への反映の有無
3	個人	対象文書 「特定歳入等及び特定歳入等に関する情報の取扱い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（案）」 該当箇所 第10「共通口座の管理」及び第11「自己点検及び外部監査」 意見 支払情報、納付情報、共通口座への入金、払込依頼、実際の払込結果その他の関係記録に不一致が生じた場合には、既存のログ、会計記録、障害管理記録等を利用し、当該不一致の発生から訂正及び解消確認までを一貫して追跡できることを、本基準又は地方税共同機構の内部規程において確保してください。 既存の規程又は管理方法によって既に確保されている場合には、原因、対応、訂正結果及び解消確認が、どの規定又は記録によって相互に接続されるのかを、意見募集結果等で示してください。 理由 基準案では、共通口座について入出金額及び残高を記録し、責任者が確認及び保管することとされています。また、障害等の原因究明、再発防止、自己点検及び外部監査も規定されています。 しかし、支払情報と実際の入金、払込依頼と払込結果、又は地方公共団体へ送信された情報の間に不一致が生じた場合に、それぞれの記録を同一案件として接続し、誰が何を根拠に解消を確認したかを追跡する機能は、公表された基準案からは確認できません。 求めるのは、新たな恒久報告制度や別個の台帳の設置ではありません。不一致が発生した場合に限り、既存の記録へ共通の管理番号又は相互参照情報を付すなど、現在の管理方法を利用して対応できるものです。 この機能を確保することで、納付済みであるにもかかわらず未納として扱われる事態、誤った口座への払込み、訂正結果が地方公共団体側へ反映されない状態等について、原因及び処理の所在が主体間を移動したまま終了することを防ぎ、同種事案が再発した場合にも過去の対応を確認できると考えます。	御意見についてはシステムに関わる点であり、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、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。以上を踏まえ本基準案の修正は行いませんが、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
4	匿名	抽象的な要件であり、より具体的なものにすることを推奨します。具体的には、我が国および世界的な標準である発生主義に基づく帳簿を漏れなく管理できることや、情報開示請求に対応できるラベリング機能が必要と考えます。	御意見にある「発生主義に基づく帳簿を漏れなく管理できること」及び「情報開示請求に対応できるラベリング機能」については、対象となる帳簿の範囲、準拠すべき基準、付与すべきラベルの内容等が具体的に示されていないため、御提案の趣旨及び必要とされる措置を明確に把握することが困難です。 以上を踏まえ、御意見を踏まえた本基準案の修正は行わず、原案のとおりとします。	無

No.	意見提出者	案に対する御意見及びその理由	御意見に対する考え方	基準への反映の有無
5	匿名	本基準案では、システムの安全性及び信頼性を確保するための対策が幅広く規定されており、重要な取組であると考えます。 その上で、以下の点について検討又は明確化をお願いしたいと思います。 1. 監査・点検について 基準が策定されても、継続的に運用状況を確認できなければ実効性が十分に確保されない可能性があります。定期的な監査や点検の実施頻度、確認方法について、可能な範囲で考え方を示していただきたいです。 2. 基準遵守の確認について 本基準を満たしているかについて、自己点検だけでなく、第三者による確認や客観的な評価の仕組みを設けることも、安全性及び信頼性の向上につながると考えます。 3. 基準違反時の対応について 基準が守られていなかった場合の改善手続や是正措置、必要に応じた公表等の考え方についても整理されると、制度全体の実効性がより高まるものと考えます。 国民が安心して地方税等のオンライン収納サービスを利用できる制度となるよう、御検討をお願いいたします。	本基準案の「第5　機構における運用管理上の安全性及び信頼性の確保」の「11　この基準の遵守並びに地方税共通納税システム、利用者用ソフトウェア及び利用者用ソフトウェア開発要件のセキュリティ対策に係る自己点検及び外部監査」では、本基準の遵守状況に関する自己点検、その結果を踏まえた改善及び外部監査について定めるとともに、その結果を総務大臣に報告することとしています。 点検及び監査の具体的な実施時期や頻度については、その目的、対象及びリスク等を踏まえ、実効性が確保されるよう適切に定められるべき事項であることから、本基準案の修正は行いませんが、いただいた御意見については、今後の運用を検討する際の参考とします。	無
6	匿名	本改正について、地方自治体の収納業務を共同化することにより、自治体職員の事務負担を軽減し、効率的な行政運営につなげようとする方向性には賛成します。人手不足が深刻化する中で、定型的な収納業務を集約することには一定の意義があると考えます。 一方で、制度を円滑かつ安全に運用するためには、情報セキュリティだけでなく、委託体制そのものの管理についても十分な配慮が必要であると考えます。 まず、委託業務が再委託、さらに再々委託へと広がる多重下請構造は、責任の所在が不明確となり、事故や情報漏えいが発生した際の原因究明や責任追及を困難にするおそれがあります。また、中間事業者が増えることで、コスト増加や業務品質の低下を招く可能性もあります。 そのため、再委託は必要最小限とし、原則として一次請けまでとすることや、それ以上の再委託を認める場合には地方税共同機構による事前承認を必要とするなど、厳格な管理を行うことを検討していただきたいと思います。 また、地方税共同機構や自治体が、実際にどの事業者が業務を実施しているのかを常に把握できる体制を整え、委託先だけでなく再委託先も含めた監査を実施できるようにすることが望ましいと考えます。委託先には、再委託先を含めた業務全体の管理責任を明確に負わせることも重要です。 さらに、安全性基準については委託先だけではなく、再委託先にも同等の基準を適用することを明文化していただきたいと考えます。個人情報や収納情報を取り扱う業務については、国外への再委託や国外でのデータ処理について慎重な対応が必要であり、原則として認めない方向で検討することを要望します。 最後に、本制度によって収納業務が効率化され、自治体職員の負担が軽減されるのであれば、その成果は人員削減や給与抑制ではなく、市民サービスの充実につなげていただきたいと思います。福祉、防災、子育て支援、窓口対応など、人手不足が課題となっている分野へ人的資源を振り向けることで、住民が制度改正の効果を実感できるものになると考えます。 本制度が、効率化だけでなく、安全性の確保と行政サービスの向上を両立する制度となることを期待しております。	本基準案では、再委託につ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。以上を踏まえ本基準案の修正は行いませんが、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
7	匿名	地方税共同機構が取り扱う地方公金収納システムは、住民の個人情報、納付情報、口座情報及び地方公共団体の公金を扱う極めて重要な社会インフラです。一度重大な情報漏えい、サイバー攻撃又はシステム障害が発生すれば、その影響は全国の地方公共団体及び住民に及びます。しかし、基準案では、国外企業、外国資本企業、外国企業が開発又は管理するシステム、国外への再委託及び国外からの保守・運用アクセスについて、十分な制限が設けられていません。 そのため、次の事項を基準として明記することを要望します。 1　国内完結を原則とすること 地方公金収納システムの設計、開発、運用、保守、監視、障害対応、データ保存及びバックアップは、日本国内で完結することを原則としてください。また、中核システムについては、日本国内に本店及び主要な運用拠点を有し、日本法の適用を受ける法人に限り委託できるものとしてください。 2　外国政府等の影響を受ける事業者の排除 外国政府、外国政府系機関、国有企業その他外国政府の実質的な支配又は影響を受ける事業者については、地方公金収納システムの中核業務を受託できないものとしてください。委託に当たっては、実質的支配者、主要株主、議決権、資金提供者及び役員構成を確認し、外国政府の影響が認められる場合には委託を認めないこととしてください。 3　国外へのデータ移転等の禁止 住民情報、納付情報、口座情報、認証情報、監査ログその他地方公金収納システムに係るデータについては、日本国外への保存、複製、バックアップ、閲覧及び処理を原則として禁止してください。国外法令に基づく情報開示請求又は国外からのアクセス要求に応じる可能性があるサービスは利用しないことを明記してください。 4　国外からの保守及び再委託の禁止 国外拠点又は国外居住者によるシステム保守、運用、障害対応、遠隔操作及び管理者権限によるアクセスは原則として禁止してください。また、国外企業又は国外拠点への再委託についても原則禁止とし、例外を認める場合には総務大臣の承認及び第三者機関による安全性審査を義務付けてください。 5　外国企業製システム等の利用 地方公金収納システムの中核部分については、外国企業が管理権限を保持するシステム、国外から更新又は遠隔操作が可能なシステム及び安全性を十分に確認できないシステムを使用しないことを原則としてください。やむを得ず利用する場合には、ソースコード、安全性評価、通信先、更新経路、遠隔操作機能、データ送信機能等について、国が指定する第三者機関による審査を義務付けてください。 6　海外で生活・勤務する日本人への配慮 一方で、海外赴任者、海外留学生、在外研究者、外交官、自衛官、船員その他海外で生活又は勤務する日本国民については、日本国内の地方税及び地方公金を円滑に納付できる環境を確保する必要があります。そのため、国外から納付手続を利用すること自体を制限するのではなく、利用者本人については、多要素認証、電子証明書等による本人確認を前提として、海外からの安全な利用を認める制度としてください。この例外は、日本国民又は日本国内法人が適法に利用する場合に限り認めるものであり、システムの運用、保守、管理、データ保存及び管理者権限についてまで国外で行うことを認める趣旨ではありません。 7　国による監査 国は、上記基準が遵守されていることについて定期的に監査を実施し、委託先及び再委託先の実態調査、ソースコード管理、国外アクセスの有無、データ保存場所及び外国政府の影響について確認してください。違反が認められた場合には、直ちに是正命令、契約解除、接続停止及び委託先変更を命ずることができる制度としてください。 結び 地方公金収納システムは国民及び地方公共団体の財産を支える重要インフラであり、その安全性は利便性より優先されるべきです。地方公共団体及び住民情報を保護するため、システムの中核部分については「国内完結」を原則とし、国外企業への委託、国外へのデータ移転、国外からの管理及び外国政府の影響を受ける事業者の関与を厳格に制限する制度を要望します。その一方で、海外で勤務・生活する日本国民が不利益を受けることのないよう、安全な本人認証を前提として国外からの納付利用を確保する制度を併せて整備することを要望します。	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

No.	意見提出者	案に対する御意見及びその理由	御意見に対する考え方	基準への反映の有無
8	匿名	地方公金の収納事務に関する安全性・信頼性の確保について、情報管理を最優先とすることを強く求めます。 税金や公金の収納には、氏名、住所、口座情報、納付状況など、国民の生活に直結する重要な情報が関係します。 公金収納のデジタル化・効率化を進める場合でも、利便性を理由に個人情報の取扱いを軽視してはなりません。 特に、システム障害やサイバー攻撃、委託先からの情報漏えいが発生した場合、誰が責任を負うのかを明確にしてください。 また、地方公共団体、地方税共同機構、金融機関、システム事業者等の間で情報が共有される場合には、情報の利用目的と共有範囲を厳格に限定すべきです。 行政の効率化のために、国民の公金情報が必要以上に集約・共有されることには反対します。 公金収納システムについては、情報の最小化、目的外利用の禁止、第三者提供の制限、アクセス権限の厳格な管理、保存期間の明確化、事故発生時の迅速な公表と救済を徹底してください。 「便利になるから」という理由だけで国民の重要情報を行政・関連機関に集中させるのではなく、国民の財産とプライバシーを守ることを最優先とする制度にしてください。	本基準案では、地方公金及びこれに関する情報の安全性及び信頼性を確保するため、情報の適切な管理、アクセス制御や障害対応、委託先及び再委託先の管理その他必要な措置を定めています。また、具体的な運用については、関係法令、「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、地方税共同機構において必要な措置を講じなければならないこととしております。 また、システムの運用に関わる点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。以上を踏まえ本基準案の修正は行いませんが、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
9	匿名	【意見内容】 地方公金の収納事務および関連情報の取り扱いにおいて、安全性及び信頼性を真に担保するため、以下の点について基準の厳格化および明確化を求めます。 外国法人の管轄下にあるクラウドサービス等の利用制限とデータソブリンティの確保 理由: 本基準案において、税務データや公金関連情報が国内のデータセンターに保管される場合であっても、その基盤を提供する企業が外国法人の場合、外国の法執行機関(例:米国のCLOUD法等)に基づくデータ強制開示命令や国外からのアクセスリスクを完全に排除することは困難です。 要望: データの保管場所だけでなく、システムの運営・管理権限を持つ事業者や親会社の資本構成・管轄法域について、外国政府の不当な介入や法執行の対象外となるような、より厳格な安全要件を明記してください。 サプライチェーン(再委託先・オフショア開発)における外資・海外アクセスの統制 理由: 一次請けの国内ITベンダーがクリアしていても、二次・三次請け以降の下請け構造や、海外のオフショア開発拠点、外国籍のエンジニアによるリモート保守等を通じて、機微な情報やシステム管理者権限が実質的に海外へ露出するリスクが懸念されます。 要望: 再委託先の選定条件や、システム開発・保守に携わる人員のセキュリティクリアランス、さらに日本国外からのアクセスを原則禁止または厳格に制限する規定を、委託先の役務基準に明文化してください。 資本構成の変化(事後買収等)に対するガバナンスと契約解除条項 理由: 契約締結時は国内資本であった受託・委託企業が、その後に外資系ファンドや海外企業に買収された場合、知らぬ間にガバナンスが変質し、セキュリティ水準が低下するリスクがあります。 要望: 契約期間中における委託先の資本構成の変化や、実質的な支配権の移転を継続的に把握・審査する仕組みを設け、安全性の基準を満たさなくなった場合の速やかな契約解除や移行を担保できる条項を盛り込んでください。	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。	無
10	匿名	地方税共同機構による地方公金の収納事務に係る安全性及び信頼性の確保に必要な基準(案)等について、以下の点を意見として提出いたします。 まず、本案には「成果目標」および「KPI(効果検証指標)」が存在しておらず、制度導入後に安全性・信頼性が向上したかどうかを客観的に確認する手段が示されていません。政府は既に全府省庁・原則全事業を対象として EBPM・行政事業レビューを実施しているため、本案件でも同様に成果目標と KPI を設定する必要があります。設定しない理由があるのであれば、その理由を明確に示してください。 以下に、本案件で必須と考えられる KPI の例を示します。 ・重大障害件数(住民・自治体に影響する障害の年間件数) ・情報漏えいインシデント件数 ・収納処理の遅延率・エラー率 ・クラウド事業者のセキュリティ監査での指摘件数 ・自治体・住民からの苦情件数(納付不可・画面停止など) これらは制度の目的である「安全性」「信頼性」「処理品質」を直接測定できる指標であり、欧米でも一般的に使用されているものです。必要であれば欧米の関係者にも確認してください。 また、これらの KPI を算出するためのデータは、以下の主体が責任を持って収集すべきです。 ・地方税共同機構:障害発生記録、処理遅延・エラー率、監査結果 ・委託クラウド事業者:システムログ、セキュリティインシデント記録、復旧時間 ・自治体:住民からの苦情件数、納付不能事例の報告 ・総務省:各主体からのデータを統合し、年次報告として公表 データは、障害ログ・監査報告・問い合わせ記録など、既存の業務で日常的に取得しているものを活用すればよく、追加の負担は最小限で済みます。記録項目を増やしすぎると誤記載や見逃しが増えるため、必要最小限の項目に絞って制度設計を行ってください。 さらに、行政手続法39条2項が求める「具体的かつ明確な内容」「題名および根拠条項の明示」について、本案は技術仕様や責任分担の詳細が抽象的であり、住民・自治体・事業者が制度の実効性を判断するには不十分です。安全性基準や委託先の役務内容が抽象的なままでは、行政の責任範囲が曖昧になり、納税者に不利益が生じる可能性があります。 行政手続法の要件を満たせていない場合は、制度の透明性と国民の信頼を確保するためにも、担当行政官の方々には「抽象的な案を公示することが納税者にとって害となる」ことを理解していただき、必要な改善を行っていただきたいと考えます。制度の明確化は行政官個人の責任追及を目的とするものではなく、国民の安全と行政の信頼性を守るための最低限の要件です。 また、本案には成果目標も KPI も存在しないため、以下の文章の趣旨を追記していただくことを求めます。 「政府が既に全府省庁・原則全事業を対象として実施している EBPM・行政事業レビューの趣旨に照らし、当該案件について成果目標及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。そして、政策効果を検証可能な成果指標、基準値、目標値及び達成期限を設定し、その実績と予算への反映状況を公表してください。」 なお、KPI は最初から完璧なものを作る必要はありません。制度導入時点では 50%程度の完成度で構いませんので、2か月または半年ごとに見直しを行う運用を提案します。未知のトラブルを事前に完全に予測することは不可能であり、継続的な改善こそが行政の信頼性を高めます。 最後に、業務経験が長期化すると「慣れ」による確認不足や手順省略が起こりやすく、事故やミスが増える傾向があることは多くの統計で指摘されています。スペーシアの事故のように、人命に関わる事例もあります。KPI による数値の増減を定期的に確認することで、危険性の兆候に早期に気づくことができ、事故防止に寄与します。 以上の理由から、本案には必ず成果目標と KPI を設定し、データ収集方法と検証方法を明確に示した上で、公表していただくことを強く求めます。	本基準案は、地方税共同機構が特定歳入等に関する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

No.	意見提出者	案に対する御意見及びその理由	御意見に対する考え方	基準への反映の有無
11	個人C	私は、減税推進・日本人ファースト・中国製品排除・中国人排除・行政事務の徹底削減を強く求め、政府の過剰な介入に断固反対する一国民として、本件基準案等に対し、以下のとおり意見を提出します。 本基準案は、地方税共同機構による特定歳入等の収納事務における安全性・信頼性確保と委託先基準を定めるものですが、国家・国民の安全を最優先すべき観点から極めて不十分である一方、自治体・事業者に過度な負担と政府の過剰介入を助長する内容です。以下、あらゆる関連問題を網羅的に指摘し、抜本的な見直しを求めます。 ### 1. 中国製品・中国人・中国関連の徹底排除を最優先せよ（日本人ファースト・安全保障の観点から） 地方公金収納は国民の税金・公金を扱う機微情報であり、中国製システム・ソフトウェア・ハードウェア・中国人技術者の関与はデータ流出・サイバー攻撃・不正アクセスのリスクを極めて高めます。 基準案で安全性・信頼性を求めるだけでは不十分です。**収納システム・情報取扱い・委託先のすべてにおいて中国製品・中国企業・中国人の関与を原則全面排除**し、日本人ファーストの立場から国内企業・日本人担当者・国内完結を絶対優先してください。中国依存を残した収納事務は国民の財産と安全保障を損なうものであり、絶対に認められません。 ### 2. 政府の過剰な介入に断固反対し、行政事務を徹底削減せよ 基準案は、情報取扱い基準や委託先への詳細な役務基準を課すものです。これは事務肥大化と過剰介入です。自治体や委託先にこれほど厳格な基準・報告を強いることは、現場の負担を増大させます。**行政事務を半減以上に削減**し、基準の最小化・ワンストップ化・デジタル完結を義務付け、官僚主導の監督を最小限にしてください。 ### 3. 減税を基盤とした国内システム・日本人人材強化を義務付けよ セキュリティ対策やシステム更新は巨額のコストを要します。法人税等の大幅減税、システム投資の即時償却・税額控除、日本人IT人材育成優遇を明記し、補助金依存をやめ、減税による民間活力を優先してください。 ### 4. その他、盛り込むべきあらゆる問題点 - 中国脅威を国際基準より上位に置き、国内完結・日本人限定を原則化。 - 行政コスト抑制と減税の両立、基準の透明化、中小・地方負担軽減。 - 少子高齢化下の国内人材維持、現場実態無視の解消。 - 過剰介入の排除（基準は必要最小限に限定）。 - データ・システムの中国リスクを前提に設計。 以上を踏まえ、中国製品排除・中国人排除・日本人ファースト・大幅減税・行政事務大幅削減・政府過剰介入反対を核心とするよう抜本見直しを求めます。これらを反映しなければ、本基準は現場を疲弊させ、地方公金の真の安全性確保と国家・国民の安全を確保できません。 意見が政策に反映されることを期待します。	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。	無
12	匿名	地方税共同機構による地方公金の収納事務は、単なる決済事務ではなく、地方公共団体に対する住民の信頼と公金管理の根幹に関わる重要な業務である。したがって、安全性及び信頼性の確保に必要な基準を定めるに当たっては、通信や機器の安全管理にとどまらず、委託先及び関係事業者の資本関係や支配関係まで厳格に確認できる制度とすべきである。現行案では、委託先となる事業者や関係する運営主体について、外資による出資、議決権保有、親会社支配、実質支配者の所在などを明確に排除又は制限する規定が見当たらず、形式上は日本法人であっても、実質的には外国資本や外国の影響下にある事業者が地方公金収納に関与し得る余地が残されている。このような状態では、地方公金に関する情報の管理、障害対応、業務継続、情報流出リスクの統制について、国民の理解と信頼を十分に得ることはできない。少なくとも、委託先及びその親会社、主要株主、実質支配者並びにシステム運用に関与する重要な事業者について、外国資本の直接又は間接の支配がある場合は委託を認めない旨を基準上明記すべきである。 また、再委託については、原則として認めるべきではない。地方公金の収納事務は、責任の所在が曖昧になること自体が大きなリスクであり、再委託が認められれば、契約上の相手方と実際の業務実施主体が分離し、監督、監査、事故時対応、情報管理の実効性が著しく低下するおそれがある。特に、再委託先や再々委託先まで含めれば、資本関係や実質支配関係の把握は一層困難となり、結果として、制度上想定していない主体が地方公金収納の実務に関与する危険が高まる。公金収納という高度の公共性を有する業務については、利便性や事務効率よりも、責任の一元化と監督可能性を優先すべきであり、委託を行うとしても一者に限定し、再委託及び再々委託は明文で禁止すべきである。やむを得ず補助的業務について例外を設ける場合であっても、収納情報、利用者情報、決済情報に接する業務、システム運用、障害対応、保守、監視等の中核業務は一切再委託を認めず、事前承認、全面開示、常時監査、違反時の即時解除を義務付ける必要がある。 以上から、本基準案には、委託先及び関係事業者に対する外資規制、実質支配者確認義務、国外支配排除規定、並びに再委託禁止規定を明記するよう強く求める。地方公金の収納は国家及び地方自治の基盤に直結するため、一般の民間決済業務と同列に扱うべきではなく、国は最も厳格な基準により制度設計を行うべきである。	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を求めています。	無
		「地方税共同機構による地方公金の収納事務に係る安全性及び信頼性の確保に必要な基準（案）等」について、以下のとおり意見を提出します。 【意見の要旨】 本基準案が、地方公金の収納に関する情報について、機密性・完全性・可用性の確保、無害化処理、通信データの暗号化、秘密鍵管理、不正アクセス対策、バックアップ、監査、委託先・再委託先管理等を詳細に規定していることを支持します。 その上で、地方公金に関する情報の安全性及び信頼性をさらに高めるため、「侵入や情報窃取そのものを防止する対策」に加えて、「仮に侵入・窃取が発生しても、取得されたデータ単体では元の情報を復元・利用することが困難となる状態を構築する」という、侵害後の被害最小化の考え方を明示することを要望します。 具体的には、暗号化に加え、秘密分散等によるデータの分散・無意味化、端末への重要データの非保持化、単一のサーバー・ストレージ・委託先等が侵害されても完全な情報を取得できない構成等を、リスクに応じて検討する技術的選択肢として基準に加えることを提案します。 また、委託先・再委託先についても、侵入防止策だけでなく、「当該事業者が侵害された場合に地方公金に関する情報を利用可能な状態で取得されるか」という観点を、委託先選定・監督・監査に取り入れることを要望します。 さらに、人的ミスを完全になくすことを前提とせず、米国国立標準技術研究所（NIST）のHuman-Centered Cybersecurityの考え方も参考に、利用者や管理者が個別に正しい判断・操作を行うことだけに依存せず、通常の業務の中で重要情報が自動的・標準的に保護される構成を重視することを提案します。 【対象となる案・該当箇所】 「特定歳入等及び特定歳入等に関する情報の取扱い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（案）」		

No.	意見提出者	案に対する御意見及びその理由	御意見に対する考え方	基準への反映の有無
		「特定歳入等及び特定歳入等に関する情報の取扱い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（案）」 ・第4「地方税共通納税システムの環境及び設備」 ・第4中「無害化処理の実施」 ・第4中「通信相手との相互認証」 ・第4中「データの暗号化」 ・第4中「秘密鍵の厳重な管理」 ・第4中「模擬攻撃に対する防御訓練の実施」 ・第5中「データ等のバックアップ」 ・第5中「不正アクセスの早期発見」 ・第5中「不正アクセスが判明した場合の対応」 ・第5中「委託を行う場合等の措置」 ・第6「他の情報システムとの接続」 及び 「特定歳入等の収納の事務を委託する場合における委託先に求める役務（案）」 【意見内容及び理由】 本基準案は、地方公金の収納という高い安全性・信頼性が求められる事務について、地方税共通納税システム、その利用者用ソフトウェア、通信、サーバー、運用保守端末、委託先等を含めた広範なセキュリティ対策を規定するものであり、その方向性を支持します。 特に、本基準案が、インターネット回線を経由して送信された支払情報発行依頼情報及び納付情報について、無害化処理を実施した上で地方税共通納税システムへ取り込むことを求めている点は重要と考えます。 外部から受け取るデータについて、単に「受信する」のではなく、安全な形式へ変換するなどして、不正プログラム等がシステム内部へ入り込むことを防止するという考え方が既に採用されています。 私は、この「無害化」という考え方を、外部から内部へ入ってくるデータだけではなく、サイバー攻撃等によって内部から外部へ窃取される可能性のある重要データの保護にも広げることが有効と考えます。 すなわち、 「危険なデータを内部に入れないための無害化」 だけではなく、 「重要なデータが外部へ窃取された場合にも、第三者にとって意味のある情報として利用させないための無意味化」 という考え方です。 【侵入防止だけでなく、侵害後の被害最小化を】 　本基準案では、ファイアウォール、相互認証、暗号化、秘密鍵管理、模擬攻撃、バックアップ、不正アクセスの早期発見等、多層的な対策が示されています。 これらはいずれも重要な対策であると考えます。 　しかし、サイバー攻撃の高度化を踏まえると、これら全てを実施した場合であっても、侵入、認証情報の窃取、未知の脆弱性の悪用、内部不正、設定ミス、委託先からの侵害等を完全に排除することは困難です。 そのため、 「どうすれば侵入されないか」 だけでなく、 「侵入された場合に何が盗まれるのか」 「盗まれたデータは、そのまま第三者が利用できるのか」 「一つのサーバー、ストレージ、端末又は委託先が侵害されただけで、完全な情報を取得できてしまわないか」 という観点を安全基準に加えることを提案します。 　地方公金の収納に関する情報は、地方公共団体、地方税共同機構、金融機関、利用者、委託事業者等の間で取り扱われるため、一つの境界だけを守れば安全性を確保できるものではありません。 　そこで、重要なデータについて、暗号化に加えて、秘密分散等によってデータを複数に分散し、各断片単体では元の情報として意味を持たない状態とすることや、業務端末に完全な重要データを恒常的に保持しない構成等についても、技術的選択肢として検討することが有効と考えます。 これは特定の製品や方式の採用を求めるものではありません。 　重要なのは、 「単一の場所が侵害された場合に、完全な情報が取得される構造になっていないか」 という観点を安全基準に取り入れることです。 【暗号化とデータの分散・無意味化の多層化について】 　本基準案では、機構サーバと地方団体サーバとの間の通信について、送信する支払情報及び納付書情報の暗号化を実施することが求められています。 また、その暗号化等に必要となる秘密鍵について、厳重に保護し、外部への漏えいを防止する措置も求められています。 これらは重要な措置ですが、本基準案自身が秘密鍵の漏えい防止を求めていることからも分かるように、暗号化の安全性を確保するためには鍵の適切な管理が不可欠です。 　そこで、暗号化を置き換えるのではなく、その上に別の防御層を加えるという観点から、重要度の高い情報については秘密分散等によるデータの分散・無意味化も選択肢として検討することを提案します。 　例えば、一つの保存領域から取得されたデータだけでは完全な情報を復元できない構成とすることで、単一障害点・単一侵害点から情報全体が漏えいするリスクを低減することが期待できます。 暗号化とデータ分散・無意味化を適切に組み合わせることで、 「通信を盗聴されても内容を保護する」 「保存領域が侵害されても完全な情報を取得させない」 という異なる層での防御が可能になると考えます。 【委託先・再委託先について】 　本基準案では、地方税共通納税システム等の開発、作成、変更、運用保守等を委託する場合、委託事業者の社会的信用及び能力を確認するとともに、本基準と同様のセキュリティ対策を実施させ、適切に監督することが求められています。 　また、再委託についても事前承認を求め、秘密保持、個人情報の持出し禁止、目的外利用禁止、漏えい時の責務、委託終了後の返却・廃棄、従事者の明確化、監督・教育、監査・調査等について契約上定めることが求められています。 この規定は非常に重要であると考えます。 一方、委託先の安全性を評価する際には、 「適切なセキュリティ対策を行っているか」 だけではなく、 「それでも侵害された場合に、どのようなデータが取得され得るか」 という観点を加えることを提案します。 委託先や再委託先が必要以上のデータを保持しないこと、業務端末等に完全な重要データを残さないこと、一つの委託先が侵害されても完全な重要情報を取得できないような構成を採用すること等は、サプライチェーンを経由した情報漏えいの被害を抑制する上で有効と考えます。 したがって、委託先の選定、契約、監督及び監査において、 ・重要データの保管場所 ・重要データの保持期間 ・端末へのデータ保持の有無		
13	個人D	【意見内容及び理由】 本基準案は、地方公金の収納という高い安全性・信頼性が求められる事務について、地方税共通納税システム、その利用者用ソフトウェア、通信、サーバー、運用保守端末、委託先等を含めた広範なセキュリティ対策を規定するものであり、その方向性を支持します。 特に、本基準案が、インターネット回線を経由して送信された支払情報発行依頼情報及び納付情報について、無害化処理を実施した上で地方税共通納税システムへ取り込むことを求めている点は重要と考えます。 外部から受け取るデータについて、単に「受信する」のではなく、安全な形式へ変換するなどして、不正プログラム等がシステム内部へ入り込むことを防止するという考え方が既に採用されています。 私は、この「無害化」という考え方を、外部から内部へ入ってくるデータだけではなく、サイバー攻撃等によって内部から外部へ窃取される可能性のある重要データの保護にも広げることが有効と考えます。 すなわち、 「危険なデータを内部に入れないための無害化」 だけではなく、 「重要なデータが外部へ窃取された場合にも、第三者にとって意味のある情報として利用させないための無意味化」 という考え方です。 【侵入防止だけでなく、侵害後の被害最小化を】 　本基準案では、ファイアウォール、相互認証、暗号化、秘密鍵管理、模擬攻撃、バックアップ、不正アクセスの早期発見等、多層的な対策が示されています。 これらはいずれも重要な対策であると考えます。 　しかし、サイバー攻撃の高度化を踏まえると、これら全てを実施した場合であっても、侵入、認証情報の窃取、未知の脆弱性の悪用、内部不正、設定ミス、委託先からの侵害等を完全に排除することは困難です。 そのため、 「どうすれば侵入されないか」 だけでなく、 「侵入された場合に何が盗まれるのか」 「盗まれたデータは、そのまま第三者が利用できるのか」 「一つのサーバー、ストレージ、端末又は委託先が侵害されただけで、完全な情報を取得できてしまわないか」 という観点を安全基準に加えることを提案します。 　地方公金の収納に関する情報は、地方公共団体、地方税共同機構、金融機関、利用者、委託事業者等の間で取り扱われるため、一つの境界だけを守れば安全性を確保できるものではありません。 　そこで、重要なデータについて、暗号化に加えて、秘密分散等によってデータを複数に分散し、各断片単体では元の情報として意味を持たない状態とすることや、業務端末に完全な重要データを恒常的に保持しない構成等についても、技術的選択肢として検討することが有効と考えます。 これは特定の製品や方式の採用を求めるものではありません。 　重要なのは、 「単一の場所が侵害された場合に、完全な情報が取得される構造になっていないか」 という観点を安全基準に取り入れることです。 【暗号化とデータの分散・無意味化の多層化について】 　本基準案では、機構サーバと地方団体サーバとの間の通信について、送信する支払情報及び納付書情報の暗号化を実施することが求められています。 また、その暗号化等に必要となる秘密鍵について、厳重に保護し、外部への漏えいを防止する措置も求められています。 これらは重要な措置ですが、本基準案自身が秘密鍵の漏えい防止を求めていることからも分かるように、暗号化の安全性を確保するためには鍵の適切な管理が不可欠です。 　そこで、暗号化を置き換えるのではなく、その上に別の防御層を加えるという観点から、重要度の高い情報については秘密分散等によるデータの分散・無意味化も選択肢として検討することを提案します。 　例えば、一つの保存領域から取得されたデータだけでは完全な情報を復元できない構成とすることで、単一障害点・単一侵害点から情報全体が漏えいするリスクを低減することが期待できます。 暗号化とデータ分散・無意味化を適切に組み合わせることで、 「通信を盗聴されても内容を保護する」 「保存領域が侵害されても完全な情報を取得させない」 という異なる層での防御が可能になると考えます。 【委託先・再委託先について】 　本基準案では、地方税共通納税システム等の開発、作成、変更、運用保守等を委託する場合、委託事業者の社会的信用及び能力を確認するとともに、本基準と同様のセキュリティ対策を実施させ、適切に監督することが求められています。 　また、再委託についても事前承認を求め、秘密保持、個人情報の持出し禁止、目的外利用禁止、漏えい時の責務、委託終了後の返却・廃棄、従事者の明確化、監督・教育、監査・調査等について契約上定めることが求められています。 この規定は非常に重要であると考えます。 一方、委託先の安全性を評価する際には、 「適切なセキュリティ対策を行っているか」 だけではなく、 「それでも侵害された場合に、どのようなデータが取得され得るか」 という観点を加えることを提案します。 委託先や再委託先が必要以上のデータを保持しないこと、業務端末等に完全な重要データを残さないこと、一つの委託先が侵害されても完全な重要情報を取得できないような構成を採用すること等は、サプライチェーンを経由した情報漏えいの被害を抑制する上で有効と考えます。 したがって、委託先の選定、契約、監督及び監査において、 ・重要データの保管場所 ・重要データの保持期間 ・端末へのデータ保持の有無	御意見についてはシステムの運用に関わる点であり、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、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。本基準案の修正は行いませんが、いただいた御意見については、今後の運用を検討する際の参考とします。	無

No.	意見提出者	案に対する御意見及びその理由	御意見に対する考え方	基準への反映の有無
		・端末へのデータ保持の有無 ・暗号化及び鍵管理 ・重要データの分散・無意味化の有無 ・単一のシステム又は事業者が侵害された場合に取得可能となる情報の範囲 ・インシデント発生時の情報漏えいの影響範囲 等について、リスクに応じて確認することを提案します。 【NISTのHuman-Centered Cybersecurityと人的リスクについて】 本基準案では、操作ミスの防止、訓練、秘密保持、従事者への監督・教育等、人的要素についても複数の対策が規定されています。 これらは重要ですが、人が常に正しい判断・操作を行うことだけを前提とした安全設計には限界があります。 米国国立標準技術研究所(NIST)は、Human-Centered Cybersecurity(人間中心のサイバーセキュリティ)の研究を進めており、2026年に公表された研究でも、サイバー侵害における人的要素を踏まえ、人の行動、限界、動機、認知バイアス、意思決定、組織文化等を考慮したセキュリティ設計の重要性が示されています。 この考え方を地方公金収納の安全対策に当てはめれば、職員や委託先の従事者が、 「この情報は重要だから暗号化する」 「このファイルは端末に保存してはいけない」 「このデータは業務終了後に削除する」 と、その都度正しく判断し続けることだけに依存するのではなく、通常の業務を行うだけで重要情報に必要な保護が自動的・標準的に適用される構成を目指すことが重要と考えます。 例えば、重要情報について保存時に自動的に保護が適用されること、業務端末に完全なデータを恒常的に保持しないこと、単一の操作ミスや設定ミスだけでは重要情報全体が漏えいしない構成とすること等が考えられます。 教育や訓練を強化することと、人の注意・判断への依存そのものを減らすことは、相互に補完する対策であると考えます。 【バックアップと情報窃取への対策について】 本基準案では、重要なファイルについて他の記憶媒体に複製し、必要に応じて別々に保管するとともに、障害発生時に速やかに地方税共通納税システムを回復できるようにすることが求められています。 これはシステムの可用性を確保する上で重要な対策です。 一方、バックアップによって防止できるのは主としてデータ消失やシステム停止による被害であり、攻撃者によって既に取得された重要情報の悪用まで防止できるものではありません。 そのため、 「データを破壊されても復旧できる」 という対策と、 「データを窃取されても利用可能な情報として取得されにくい」 という対策を組み合わせることが重要と考えます。 地方公金の収納を支えるシステムでは、可用性だけでなく、情報そのものの機密性を侵害後まで維持するという観点も重視していただきたいと考えます。 【提案】 以上を踏まえ、本基準案及び委託先に求める役務について、次の考え方を明示することを要望します。 1. 侵入防止・検知・復旧に加え、「侵入・窃取が発生した場合にも重要データを利用可能な状態で取得させない」という被害最小化の観点を追加すること。 2. 重要度の高い情報について、暗号化に加え、秘密分散等によるデータの分散・無意味化、端末への重要データの非保持化等を、リスクに応じて検討可能な技術的選択肢として例示すること。 3. 単一のサーバー、ストレージ、端末、クラウド環境又は委託先等が侵害された場合、それだけで完全な重要情報を取得できる構成となっていないかを確認する観点を加えること。 4. 委託先・再委託先の選定、契約、監督及び監査において、侵入防止能力だけでなく、侵害された場合に取得されるデータの範囲及び利用可能性を評価すること。 5. 人的ミスを完全になくすことを前提とせず、NISTのHuman-Centered Cybersecurityの考え方も参考に、利用者・管理者・委託先従事者の注意や個別判断への依存を減らし、通常の業務の中で重要情報が自動的・標準的に保護される設計を促すこと。 6.「外部から入ってくる危険なデータを無害化する」という本基準案の考え方に加え、「外部へ窃取された重要データを第三者にとって利用困難な状態とする」というデータの無意味化・耐侵害性の考え方についても、安全性及び信頼性を確保するための選択肢として位置付けること。 地方公金の収納は、国民・住民と地方公共団体、地方税共同機構、金融機関、委託事業者等を結ぶ社会的に重要な仕組みです。 その安全性を「侵入されないこと」だけに依存させず、侵入、内部不正、人的ミス、委託先侵害等が発生した場合にも、重要なデータそのものへの被害を最小化できる多層的な構造とすることが、地方公金収納に対する国民の信頼を高めることにつながると考えます。		

No.	意見提出者	案に対する御意見及びその理由	御意見に対する考え方	基準への反映の有無
14	匿名	本基準案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、および地方公金の収納における過度な効率化・デジタル化推進が招く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、地方税や公金の収納事務において、効率化やシステム化ばかりを優先し、対面窓口や紙の納付書、現金決済といった物理的な決済手段を縮小・廃止へと向かわせるような基準設定への強い批判です。スマートフォンやデジタル機器の扱いに不慣れな高齢者や、通信環境を整える余裕のない生活困窮者を置き去りにする「デジタル難民」の発生は、社会的な格差と分断をさらに悪化させるものであり断じて容認できません。 第二に、行政や総務省が最優先で取り組むべきは、形骸化した効率化や事業者側の利便性追求ではなく、誰もが差別なく公平に社会手続を行えるセーフティネットの死守です。どのような生活環境にあっても、手続きの選択肢（電話や対面、現金等の物理的手段）が担保され、過度な負担なく安心して暮らせる公平な社会基盤の維持・管理へと直ちに政策の舵を切ることを強く求めます。	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、本基準案は地方税共同機構が特定歳入等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

【提出意見　14件】 上記の他、案とは無関係の御意見と判断し、提出意見として扱わなかったものが2件ありました。