地方公共団体における
個人情報利用パブリッククラウドサービス活用ガイドライン
（β版）

注意：本書はβ版であり、記載内容はすべて検討段階のものです。
APPLIC においてどのような検討がなされているかを広報することが目的であり、記載内容は決定されたものではなく、一切拘束性はありません。
本書は APPLIC クラウド・データ利活用検討 TF における 2018 年度検討内容をもとに作成されています。最終的な決定稿については 2019 年度末までの完成を目指して作業を継続しています。

2019 年 10 月 3 日

一般財団法人全国地域情報化推進協会

目次

1　初めに

1.1　対象

本ガイドラインは以下の条件を満たすパブリッククラウドサービス[1]を対象とする。

- 主に地方公共団体向けに提供されるサービスであること
- 主にパーソナルデータ[2]を取り扱うサービスであること
- 地方公共団体とネットワーク接続するに際しては LGWAN-ASP を仲介するサービスであること

エンドユーザーが住民であっても、地方公共団体が契約主体となり住民に機能を利用させるような場合も検討対象とする。例えば、パブリッククラウドサービス提供者より提供される「電子母子手帳サービス」を地方公共団体が委託契約等で調達し、住民に利用させる場合などがこれにあたる。この場合、電子母子手帳サービスに保管される利用者やその子供に関する個人情報は利用者（住民）本人によって登録されるもののみであり、地方公共団体側（職員）からの登録が一切なかったとしても、当該サービス上では地方公共団体の保有個人情報と解釈される可能性があるためである。

さらに、非識別加工情報を扱うサービスについても地方公共団体内にあっては引き続き個人情報であることから対象とする。

なお、個人情報やパーソナルデータを利用しないパブリッククラウドサービスに関しては、必要な安全性水準が比較的低い場合が想定され、取り扱いについて一貫した基準を設ける必然性が低いことから本ガイドラインの対象外とする。

1.2　背景

デジタル・ガバメント推進方針（平成 29 年 5 月 30 日高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議決定）において「【方針２－３】プラットフォームの共用化と民間サービスの活用」がうたわれ、自前主義からの脱却が明言された。ここでは「全ての機能を行政自らが構築すると いう自前主義に拘泥するのではなく、民間クラウドや民間サービスを積極的に活用し、行政機関が全てを保有・管理する形態から必要なものを必要な期間だけ利用するという考え方へ転換する」とされ、パブリッククラウドサービスの積極的活用が言及されている。

さらに、地域 IoT 実装推進タスクフォース地域資源活用分科会報告（平成 29 年 5 月 24 日 総務省 地域 IoT 実装推進タスクフォース地域資源活用分科会）においては、「クラウドファーストの原則」が、また、デジタル・ガバメント実行計画（平成 30 年 1 月 16 日 e ガバメント閣僚会議決定）では、「クラウド・バイ・デフォルト」が提唱されたところである。

このように地方公共団体におけるパブリッククラウドサービス活用は必須の状況であ

---

[1] **2 定義** 参照

[2] 「パーソナルデータの利用・流通に関する研究会報告書」［総務省 パーソナルデータの利用・流通に関する研究会，2013］の定義に従い、個人識別性を有する「個人情報」に限定することなく、広く「個人に関する情報」を「パーソナルデータ」と定義する

る。特に AI 等の最新技術を積極的に活用すべきとする観点や、CivicTech、GovTech などの新しい行政サービスの在り方との連携を推進する観点などからも、パブリッククラウドサービスを柔軟かつ安全に活用する能力が強く求められている。

一方で、パブリッククラウドサービス活用においては、従来の庁内システムや、地方公共団体専用の自治体クラウドとは異なった難しさが存在する。パブリッククラウドサービスでは、データ処理は物理的には庁外において実行される。また、パブリッククラウドサービスの多くはインターネットと接続された環境にある。さらには民間との共同（共有）環境ともなりうる。そして、地方公共団体からの制御範囲は限定的であり、全権を掌握することもできない。

1.3 目的

上記の背景を鑑み、本ガイドラインは、地方公共団体がパブリッククラウドサービスを利用するに際し、地方公共団体ならびにパブリッククラウドサービス提供者双方に以下の便益を提供することを目的とする。

1.3.1 パブリッククラウドサービス利用に際する共通認識の提供

パブリッククラウドサービスの真価を発揮させるには、多彩な活用と変化への柔軟な対応が必要になる。パブリッククラウドサービスは多種多様である。そこで、その特性を生かすには、利用者はうまくサービスを組み合わせ、多彩に活用する必要がある。一方で、社会情勢の変化や住民ニーズの変化等に応じて短期間に新たなサービスが生まれ消えていく特性を持つ。よって、利用者側にも変化へ柔軟に対応する能力が求められる。

多彩な活用と変化への柔軟な対応を可能とするには、地方公共団体とパブリッククラウドサービス提供者の双方に一定の共通認識が形成されていることが望ましい。利用者は、新しいサービスの採用を検討するたびに一からすべてを調査・評価するのは非効率である。一定の共通認識があればそのような手間を削減できる。また、多くのパブリッククラウドサービスから最適なサービスを選定するに際しても、一定の認識を共有したサービスが広まれば選択肢を豊かにすることができる。提供者にとっても、地方公共団体の調達基準に合致するための共通認識が事前に明確になっておれば事業機会を広めることができる。

本ガイドラインではこの共通認識を形成するため、パブリッククラウドサービス活用時に準拠すべき**アーキテクチャ**と、そのアーキテクチャを前提に、パブリッククラウドサービスと地方公共団の業務システムとが連携する際に参照すべき**基本ルール**を提供する。

1.3.2 パブリッククラウドサービスを安全に利用するための基準の提供

地方公共団体が安全にパブリッククラウドサービスを利用するには特有の注意すべき事項が存在する。自庁から利用するにはネットワークを介して外部接続することが当然に必須であり、全体としてのセキュリティ管理が必要となる。また、パブリッククラウドサービスは提供者によって管理され、その制御下にある。通常、利用者である地方公共団体が直接かつ完全に支配することはできない。よって、品質その他について責任をもって利用するには相応の対応が求められる。さらに、変化の激しいサービスゆえに、事業撤退やサービス内容変更などの事態への備えも必須となる。

特有の注意事項が存在する一方で、多様なサービスを多彩かつ柔軟に利用できるパブリッククラウドサービス活用においては、機能の分析・評価を行った後から利用環境の整備に取り組むことは実運用までに時間を要するために現実的ではない。地方公共団体が情報システムを利用する際のセキュリティ上の対応要件は、「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(平成 30 年 9 月版)[総務省, 2018]」や、「地方公共団体における情報セキュリティ監査に関するガイドライン(平成 30 年 9 月版)[総務省, 2018]」に整理されている。原則これらのガイドラインに則りセキュリティポリシーを作成し、必要な監査を行う必要がある。しかしながら、パブリッククラウドサービスの利用に適した形に短時間でこれらの対応を行うには相応の工夫が必要となる。

そこで、本ガイドラインでは、地方公共団体がパブリッククラウドサービスの調達を行う際に、必要な対応を効率的に実施できるよう、地方公共団体向けパブリッククラウドサービスが満たすべきセキュリティ等の水準を整理し**評価基準**としてまとめる。この評価基準に基づく確認を基本として調達を行うことで一定水準の安全性を確保可能とする。

2　定義

本ガイドラインでは以下の用語を利用する。

「なければならない」

本ガイドラインに従ったものとみなされるためには必ず対応しなければならない事項。

「してはならない」

本ガイドラインに従ったものとみなされるためには決して行ってはならない事項。

「推奨する」

本ガイドラインに従ったものとして可能な限り対応すべき事項。

「してもよい」

対応していることが本ガイドラインへの準拠に影響しないことを特に明言している事項。

以下の定義は「政府情報システムにおけるクラウドサービスの利用に係る基本方針」[各府省情報化統括責任者（ＣＩＯ）連絡会議, 2018]に準じる。

「パブリッククラウドサービス」

任意の組織で利用可能なクラウドサービスであり、リソースは事業者（クラウドサービス提供者）によって、制御されるもの。

「IaaS」

利用者に、CPU 機能、ストレージ、ネットワークその他の基礎的な情報システムの構築に係るリソースが提供されるもの。利用者は、そのリソース上に OS や任意機能（情報セキュリティ機能を含む。）を構築することが可能である。

「PaaS」

IaaS のサービスに加えて、OS、基本的機能、開発環境や運用管理環境等もサービスとして提供されるもの。利用者は、基本機能等を組み合わせることにより情報システムを構築する。

「SaaS」
利用者に、特定の業務系のアプリケーション、コミュニケーション等の機能がサービスとして提供されるもの。具体的には、政府外においては、安否確認、ストレスチェック等の業務系のサービス、メールサービスやファイル保管等のコミュニケーション系のサービス等がある。政府内においては、府省共通システムによって提供される諸機能や、政府共通プラットフォーム上で提供されるコミュニケーション系のサービス・業務系のサービスが該当する。

3　アーキテクチャ

地方公共団体が庁内システムと連携させてパブリッククラウドサービスを利用する場合、以下のアーキテクチャに従う形態をとらなければならない。
なお、インターネット側の利用者は存在しない構成もありうる。また、地方公共団体側とのネットワーク接続が存在しない構成（インターネット側利用者のみ）もありうる。

全体アーキテクチャは（図 1）の通りとする。

「基幹システム」
地方公共団体の行政システムそのもので、自治体クラウドやプライベートクラウド、オンプレミス環境に実装されていることを前提とする。これらは既存環境である。地域情報プラットフォーム標準仕様に規定されている業務に関する業務システムは、地域情報プラットフォーム標準仕様に準拠していなければならない。

「中間層」
基幹システムからパブリッククラウドサービスまでの経路に相当する。通信ネットワークだけではなく流通する情報の制御やトラストの確立などを担当する。中間層は LGWAN ASP として実装されなければならない。

「サービス層」
パブリッククラウドサービスの本体であり、実際のサービスを提供する。住民向けサービスや職員向けサービスの提供が考えられる。サービス層で実装されるサービスは次の IaaS/PaaS 層を利用して構築してもよい。

「IaaS/PaaS 層」
パブリッククラウドサービスの実装環境として提供される IaaS/PaaS を指す。サービス層の提供者（ソリューションベンダ）とは別の事業者（クラウドベンダ）によって提供される場合が多い。ファシリティや OS、ミドルウエアレベルでのセキュリティ要件などの多くはこの IaaS/PaaS 層で実装してもよい。ただし、サービス層がすべての機能を独自に実装し IaaS/PaaS 層を持たない構成としてもよい。

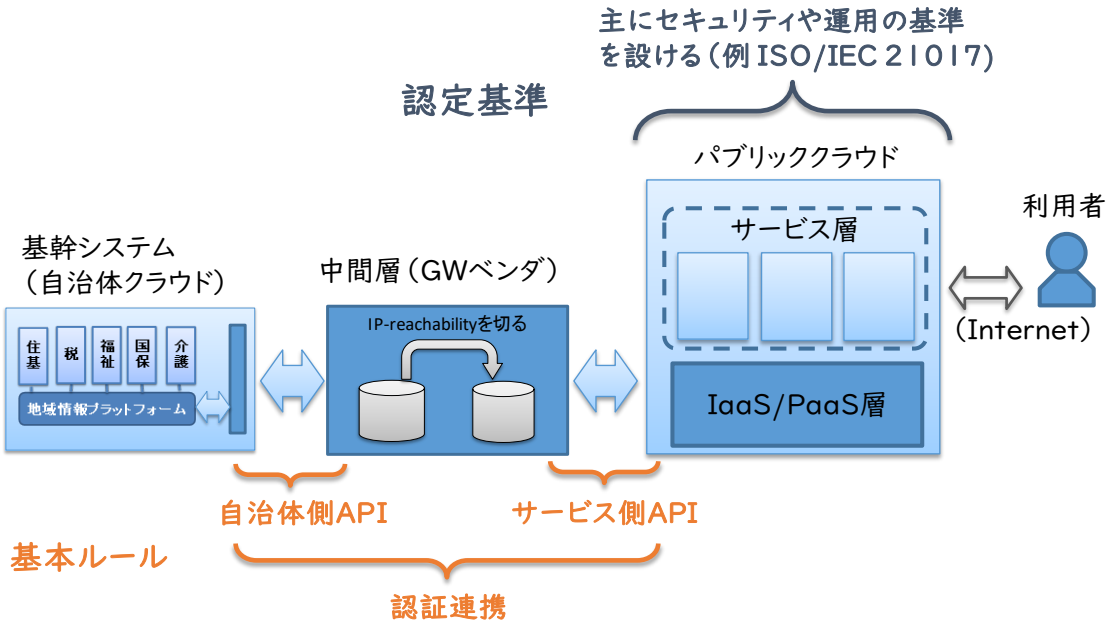

図 1 クラウドサービスアーキテクチャ

地方公共団体に対してパブリッククラウドサービスを提供する事業者は以下のいずれかの形態をとらなければならない。

① 単独提供者がサービス層、IaaS/PaaS 層の全機機能を提供する
② IaaS/PaaS 層機能のみを提供し、サービス層機能は他提供者に依存する
③ サービス層機能のみを提供し、IaaS/PaaS 層機能は他提供者に依存する

4 基本ルール

上記アーキテクチャを前提として、以下の要素について基本ルールを定める。

「自治体側 API」

基幹系システムと中間層をつなぐ API。

「サービス側 API」

中間層とサービス層をつなぐ API。

「認証連携（職員）」

サービス層が提供するサービスを利用する際の認証（認可）のための仕組み。基幹システムや庁内での職員認証基盤と連携し、シングルサインオンなどを実現する。

「認証連携（住民）」

サービス層が提供するサービスを利用する際の認証（認可）のための仕組み。住民が利用している各種認証基盤（ソーシャルログインなど）との連携機能。公的個人認証（マイナポータル）との連携も考えられる。

表 1 自治体側 API、認証連携（職員）基本ルール

No	項目	No	内容
1	サイト、サービス認証		LGWAN 利用につき規定なし
2	利用者認証、認可		LGWAN 利用につき規定なし
3	認証連携		LGWAN 利用につき規定なし
4	通信プロトコル	1	暗号化通信でなければならない。LGWAN では通信はすでに暗号化されているが、必要に応じて SSL/TLS による暗号化を行うこと
5	ネットワークセキュリティ	1	以下の経路をとること LGWAN接続ルータ→LGWAN側FW→アプリケーションサーバLGWANセグメント→FW→ゲートウエイサーバ→FW→アプリケーションサーバ（インターネット側）→FW（※LGWAN-ASPガイドライン準拠）

表 2 サービス側 API、認証連携（住民）基本ルール

No	項目	No	内容
1	サイト、サービス認証	1	EV SSL 証明書の導入を推奨する
2	利用者認証、認可	1	ID/パスワードを利用してもよい
		2	OAuth2.0 認可フレームワークを推奨する
3	認証連携		
4	通信プロトコル	1	REST（Richardson Maturity Model Level2 相当 ）を推奨する
		2	SOAP（SOAP 1.1 and Basic Profile 1.0）を利用してもよい
		3	アプリケーション層プロトコルとして HTTPS(HTTP over TLS)を推奨する
		4	HTTP/1.1 を推奨する
		5	HTTP/2.0 を利用してもよい
		6	TLS1.1 あるいは TLS1.2 を推奨する
		7	TLS なしの HTTP を利用してはならない
5	ネットワークセキュリティ	1	専用線（広域イーサあるいは IP-VPN）を推奨する ※インターネット回線（SSL-VPN 等によりセキュリティが確保された通信が保証されたもの）の活用については総務省等の検討状況に合わせて定義する
6	日本語プロファイル	1	JIS X 0213:2004 を推奨する（サービス特性ごとの拡張を検討する）
7	利用コード体系	1	地域情報プラットフォーム標準仕様自治体業務アプリケーションユニット標準仕様コード辞書 に準拠することを推奨する
		2	文字符号化スキームとして UTF-8 を推奨する（BOM は規定しない）
8	データ形式	1	JSON を推奨する
		2	XML を推奨する
		3	SOAP を利用する場合、メッセージ形式は地域情報プラットフォーム標準仕様プラットフォーム通信標準仕様に準拠することを推奨する
		4	CSV を利用してもよい

5　パブリッククラウドサービスの評価

地方公共団体がパブリッククラウドサービスを調達するに際して、確認・評価すべき事項とその評価基準を定める。

パブリッククラウドサービスを利用してパーソナルデータを処理する場合、上述のアーキテクチャ、基本ルールに従うことを前提に、以下の評価基準を満たすサービスを調達しなければならない。そのために以下の評価基準について調達要件として明確に定義しなければならない。

評価基準を満たしていることを確認するには、地方公共団体が直接評価する場合と外部機関に評価を委任する場合が考えられる。さらに、調達時のみではなく、評価基準を満たしていることを定期的に監査することが望ましい。

なお、評価基準を満たしていることを個々に確認することに代えて、ISO/IEC27017、ISO/IEC27018、CS ゴールド等を取得済みであることを確認する方法も可能とする。前述の基準を取得したサービスに関しては以下の評価基準はすべて充足しているものと判断し、個別の評価確認を不要とする。

6　評価基準

パブリッククラウドサービス提供者は地方公共団体向けにパーソナルデータを処理するサービスを提供するに際して、以下に定義する評価基準を満たすよう努力しなければならない。また、評価基準を満たしている場合、その旨を明示しなければならない。

「アーキテクチャ」に規定する以下のどの形態をとるかによって、評価基準の満たし方に複数の方式が考えられる。

① 単独提供者がサービス層、IaaS/PaaS 層の全機機能を提供する
② IaaS/PaaS 層機能のみを提供し、サービス層機能は他提供者に依存する
③ サービス層機能のみを提供し、IaaS/PaaS 層機能は他提供者に依存する

Type①の場合、すべての評価基準を単独提供者たるパブリッククラウドサービス提供者が満たしている必要がある。

Type②の場合、評価基準のうち IaaS/PaaS 層評価基準となっている部分のみ満たす必要がある。

Type③の場合、評価基準のすべてが IaaS/PaaS 層提供者とサービス層提供者のいずれかによって満たされていれば良い。サービス層提供者はサービスの提供に際して利用する IaaS/PaaS 層サービスを明示するとともに、評価基準のうち、IaaS/PaaS 層に依存する部分について明示しなければならない。

いずれの方式においても、利用者（自治体）と各階層のサービス提供者間の責任分担について事前に明確化しなければならない。責任共有のモデルを確立させたうえで、その分担に従い以下の評価基準を満たす必要がある。

表 3 IaaS/PaaS 層評価基準

1 情報セキュリティ		
1	運用・マネジメント	1 情報セキュリティマネジメントを実現するに十分な体制を持たなければならない 2 明確な情報セキュリティマネジメント手順を持たなければならない 3 リスクアセスメント等情報セキュリティマネジメントを継続的に維持する仕組み・体制を持たなければならない 4 情報セキュリティインシデントへの対応が整理されてなければならない
2	物理的セキュリティ（ファシリティ）	1 情報資産が適切に管理されていなければならない 2 ファシリティが国内になければならない 3 入退場管理等必要なセキュリティ措置が取られていなければならない 4 自然災害等に対する十分な対応がなされていなければならない
3	物理的セキュリティ（ネットワーク）	1 ファイアウオールを設置しなければならない 2 Web アプリケーションファイアウオールを設置しなければならない
		3 侵入検知、侵入防御システムを設置しなければならない 4 多重化等事業性属性に配慮した対応がなされていなければならない
4	技術的セキュリティ	1 コンピュータの管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じていなければならない
5	人的セキュリティ	1 責任者を明確にし、組織体制を構築していなければならない 2 従業員に対する教育・訓練が適切に実施されていなければならない

		3 適切なアカウント管理がなされていなければならない 4 適切なアクセスコントロールがなされていなければならない
2 性能・サービス品質		
1	性能	1 性能に関するモニタリングの仕組みを持たなければならない 2 業務継続性を担保する仕組みを持たなければならない 3 十分な拡張性を持たなければならない
2	サービスレベル	1 SLA が提示されていなければならない
3 事業		
1	経営	1 法人格を持っていなければならない 2 提供されるサービスの遂行に足りる十分な財政基盤を持ち健全な経営を行っていなければならない
2	事業継続性	1 事業継続計画を策定していなければならない 2 サービス変更・終了時の事前通告に関する取り決めを持たなければならない 3 サービス変更・終了時の代替サービス紹介等の対応策が提示されていなければならない
3	コンプライアンス	1 法令を遵守していなければならない 2 コンプライアンス担当役員を置き、必要な組織体制をもっていなければならない 3 個人情報保護指針を策定していなければならない 4 情報セキュリティ方針を策定していなければならない 5 問い合わせ、苦情窓口が設置されていなければならない 6 日本国内法が適応されるサービスでなければならない 7 利用規約等で国外法の適応を求めないサービスであることを推奨する

		8　利用する自治体の条例が適応される、あるいは条例の規定に従うサービスであることを推奨する 9　第一審管轄裁判所について利用者、提供者双方が合意可能でなければならない
4	賠償責任の明示	1　利用者に損害等発生時における賠償責任について責任範囲が明示されなければならない 2　賠償責任について利用者、提供者双方の合意が形成されなければならない
5	知的財産権	
6	監査権限	

表 4 サービス層認定基準

1 情報セキュリティ		
1	運用・マネジメント	1 情報セキュリティマネジメントを実現するに十分な体制を持たなければならない 2 明確な情報セキュリティマネジメント手順を持たなければならない 3 リスクアセスメント等情報セキュリティマネジメントを継続的に維持する仕組み・体制を持たなければならない 4 情報セキュリティインシデントへの対応が整理されていなければならない
2	人的セキュリティ	1 責任者を明確にし、組織体制を構築していなければならない 2 従業員に対する教育・訓練が適切に実施されていなければならない 3 適切なアカウント管理がなされていなければならない 4 適切なアクセスコントロールがなされていなければならない
2 分離		
1	インターネットとの接続	1 インターネット領域との接続は必要な通信のみ許可するよう適切に制御し、分離しなければならない。 ※分離の要件については総務省等の検討に合わせて改めて設定する。
2	クラウド内での環境分離	1 パブリッククラウドにおける他の情報資産とは明確に区分し、利用しなければならない。 ※他の情報資産との区分の要件については総務省等の検討に合わせて改めて設定する
3 プライバシー		
1	透明性の確保	1 個人情報の利用について具体的情報が開示されていなければならない 2 本人からの個人情報の利用停止、削除等の申し出に対応できる仕組みを要さなければならない
2	利用目的の制限	

		1 個人情報の利用目的、処理内容が明確でなければならない 2 個人情報の利用目的、処理内容が明示されていなければならない 3 目的外利用を禁止し、適切に利用目的を制限、制御する仕組みを持たなければならない
3	情報の最小化	1 処理に対して不要な個人情報を収集しないよう制御されていなければならない 2 処理内容に対して必要な個人情報のみ扱っていなければならない
4	正確性の確保	1 個人情報の正確性を確保するための仕組みを導入していなければならない 2 本人からの申し出など個人情報の修正依頼があった場合適切に対応できなければならない
5	機密性と完全性の確保	1 個人情報の機密性、完全性を保証するための仕組みを導入していなければならない 2 個人情報の利用者を適切に管理していなければならない（アカウント管理） 3 個人情報に対するアクセスコントロールを適切に実施できなければならない 4 個人情報へのアクセスに関する監査証跡を保持していなければならない 5 第三者提供を禁止し、適切に管理する仕組みを持たなければならない
6	データ削除	1 不要となった個人情報を適切に削除し、削除されたことを保証できなければならない
7	本人の参画	1 必要に応じて個人情報の利用に対する本人同意を取得する仕組みを有しなければならない

		2 本人からの個人情報利用状況に関する開示請求に応える仕組みを有しなければならない 3 本人からの申し出に基づく個人情報の修正、削除に対応する仕組みを有しなければならない（再掲）
4 性能・サービス品質		
1	性能	1 性能に関するモニタリングの仕組みを持たなければならない 2 業務継続性を担保する仕組みを持たなければならない 3 十分な拡張性を持たなければならない
2	サービスレベル	1 SLA が提示されていなければならない
5 事業		
1	経営	1 法人格を持たなければならない 2 提供されるサービスの遂行に足りる十分な財政基盤を持ち健全な経営を行っていなければならない
2	事業継続性	1 事業継続計画を策定しなければならない 2 サービス変更・終了時の事前通告に関する取り決めを持たなければならない 3 サービス変更・終了時の代替サービス紹介等の対応策が提示されていなければならない 4 サービス終了時のデータ継続性（データポータビリティ）を保証しなければならない
3	コンプライアンス	1 法令を遵守していなければならない 2 コンプライアンス担当役員を置き、必要な組織体制を持たなければならない 3 個人情報保護指針を策定していなければならない 4 情報セキュリティ方針を策定していなければならない 5 問い合わせ、苦情窓口が設置されていなければならない

参照文献

各府省情報化統括責任者（ＣＩＯ）連絡会議. (2018). 政府情報システムにおけるクラウドサービスの利用に係る基本方針.

総務省. (2018). 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(平成 30 年 9 月版).

総務省. (2018). 地方公共団体における情報セキュリティ監査に関するガイドライン(平成 30 年 9 月版).

総務省 パーソナルデータの利用・流通に関する研究会. (2013). パーソナルデータの利用・流通に関する研究会報告書 ～パーソナルデータの適正な利用・流通の促進に向けた方策～.