政府情報システムにおける
クラウド設置場所等に関する考え方

2020 年 6 月

西村 毅[1]、**満塩 尚史**[1]、**細川 努**[1]、**楠 正憲**[1]、**田丸 健三郎**[1]、**梅谷 晃宏**[1]

要旨

「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」（平成 30 年 6 月 7 日 CIO 連絡会議決定）において、政府情報システムにおけるクラウドの利用は、国内データセンタと我が国に裁判管轄権があるクラウドサービスを原則としながら、「データの保存性、災害対策等からバックアップ用のデータセンタが海外にあることが望ましい場合、又は争訟リスク等を踏まえ海外にあることが特に問題ないと認められる場合はこの限りではない」としている。本文書は、政府情報システムが高度化、複雑化するパブリック・クラウドの利用を検討する際において、クラウドサービスが「海外にあることが特に問題ないと認められる場合」の考え方を、「利用者データの可用性」、「業務サービスの継続性」、「データ保護」、「争訟リスク」の各々の観点から整理したものである。

[1] 政府 CIO 補佐官

目次

１　はじめに

１．１　背景と目的

パブリック・クラウドの進化に伴い、クラウドサービス提供者が提供する様々なマネージドサービスが増加しており、また、非常に高度化、複雑化しています。

一方、政府情報システムにおいては、「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」（平成 30 年 6 月 7 日 CIO 連絡会議決定）において、クラウドサービスの選定時に満たす事項として、「クラウドサービスに保存される利用者データの可用性の観点から、我が国の法律及び締結された条約が適用される国内データセンタと我が国に裁判管轄権があるクラウドサービスを採用候補とする。ただし、データの保存性、災害対策等からバックアップ用のデータセンタが海外にあることが望ましい場合、又は争訟リスク等を踏まえ海外にあることが特に問題ないと認められる場合はこの限りではない」としています。

本文書は、政府情報システムが高度化、複雑化するパブリック・クラウドの利用を検討する際において、当該箇所に関連するクラウドサービスの設置場所等の考え方をディスカッションペーパーとして取りまとめたものです。

１．２　用語

本文書において使用する用語は、表１-1 及び本文書に別段の定めがある場合を除くほか、標準ガイドライン群用語集の例によります。その他専門的な用語については、民間の用語定義を参照してください。

表　1-1　用語の定義

用語	意味
パブリック・クラウド	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。
IaaS（Infrastructure as a Service）	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（Platform as a Service）	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

用語	意味
	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（Software as a Service）	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。

２　設置場所に関する基本的な観点

政府情報システムは、クラウドサービスに保存される利用者データ（利用者が作成・管理するデータ）の可用性の観点から、我が国の法律及び締結された条約が適用される国内データセンタと我が国に裁判管轄権があるクラウドサービスを採用候補とすることを原則としながら、国内データセンタであることを必要とするかしないかを、以下の観点から検討することが求められます。以下の全ての観点において条件が満たされる場合のみ、クラウドサービスを国内データセンタに限定する必要がないと考えられます。

２．１　利用者データの可用性の観点

クラウドサービスに保存される利用者データの可用性が必要とされない場合、もしくは利用者データのバックアップが取得されている等の可用性が保証される場合。

２．２　業務サービスの継続性の観点

大規模災害時等に数日程度の一定期間の業務サービスの停止が許容されるなどの業務サービスの継続性が必要とされない場合、もしくは継続性が保証される場合。

２．３　データ保護の観点

クラウドサービスに保存される利用者データが公開可能情報である等の利用者データの保護が必要とされない場合、もしくは利用者データが暗号化する等の利用者データの保護が保証される場合。

２．４　争訟リスクの観点

日本国内法への準拠要否、裁判管轄等、具体的な争訟リスクが予見されない場合。

３　具体的な検討

３．１　IaaS/PaaS の検討

1)利用者データの処理や保管を行うサービス（利用者データ取扱サービス）

仮想サーバサービス、データベースサービス、ストレージサービス、マイクロサービス等と呼ばれるクラウドサービスにおいては、利用者データを直接的に処理し、または保管します。（以下、「利用者データ取扱サービス」といいます。）

利用者データ取扱サービスについては、国内データセンタの選択を前提にする必要があり、国内データセンタ以外の利用については、以下の観点からリスク管理が可能か否かを慎重に検討する必要があります。

(1) 利用者データの可用性の観点から、利用者データを保管するサーバを設置するデータセンタについては国内であることが強く望まれますが、複製された利用者データ、サービスの管理データ、システムデータ等を保管するサーバのデータセンタについては、利用者データの可用性の観点からは、国内である必要はありません。

(2) 利用者データの可用性を高めるため、日本を含む国内外の複数国のデータセンタの複数のサーバによる処理の分散が図られている場合については、利用者データの可用性の観点からは、国外であることの問題は特に生じない、むしろ可用性が向上する可能性があると考えられます。ただし、複数国に日本が含まれない場合については、日本以外の複数国のデータセンタのすべてのサーバが同時に利用できなくなる場合や国外とのネットワークがすべて途絶した場合には利用者データにアクセスできなくなりますので、複数のサーバによる可用性の向上と併せて、そのリスクを総合的に評価することが必要です。

(3) 業務サービス継続性の観点から、クラウドサービスを提供するサーバを設置するデータセンタについては国内であることが強く望まれますが、業務サービスの継続性を高めるために、日本を含む国内外の複数国のデータセンタの複数のサーバによるサービスの分散が図られている場合については、業務サービス継続性の観点からは、国内以外のデータセンタであることの問題は特に生じない、むしろ継続性が向上する可能性があ

ると考えられます。ただし、複数国に日本が含まれない場合については、日本以外の複数国のデータセンタのすべてのサーバが同時にサービス提供できなくなる場合や国外とのネットワークがすべて途絶した場合には業務サービスが継続されなくなりますので、複数のサーバによる継続性の向上と併せて、そのリスクを総合的に評価することが必要です。

(4) データ保護の観点からは、要保護情報については、複製された利用者データも含め、「電子政府推奨暗号リスト」に記載された暗号化のアルゴリズムを使用し、暗号化を行ったうえで保管されることが原則となります。利用者データについては、利用者業務データ（利用者が作成、又は収集し、業務遂行のために利用するデータ）、利用者属性データ（利用者の属性を示すデータであり、ID 等の単独で利用者を特定できないものは除く）、その他利用者データ（利用者業務データ、利用者属性データ以外の設定値やログ等に含まれる利用者データ）の各々について、開示可能なデータ（名刺や Web サイトで開示されているもの等）か開示不可なデータかを検討の上、要保護情報を整理する必要があります。要保護情報については、以下の２つの条件を満たして機密性が確保されていれば、データ保護の観点からは、国内データセンタである必要はありません。

ア）「CREPTREC 暗号リスト（電子政府推奨暗号）」に掲載されている暗号化アルゴリズムによって暗号化されている。

イ）暗号化鍵が利用者側の環境で管理されているか、もしくは、暗号化鍵がクラウドサービス内の耐タンパー装置（ハードウェアセキュリティモジュール）等の仕組みによって安全に管理され、その暗号化鍵の使用可否が利用者側の管理下に置かれる等、利用者側の意に反した復号を行うことができない仕組みが確立されている。

2)利用者データの処理や保管を行わないサービス（運用管理サービス）

利用者データを直接的に処理・保管せず、サービスの管理データやシステムデータ等のみを取扱う運用管理系のサービスを「運用管理サービス」と位置付けます。

運用管理サービスについては、国内データセンタの選択を前提にする必要があり、国内データセンタ以外の利用については、以下の観点からリスク管理が可能か否かを慎重に検討する必要があります。

(1) 業務サービス継続性の観点から、運用管理サービスを提供するサーバを設置するデータセンタについては国内であることが望まれますが、シス

テムの可用性を高めるために国外のデータセンタも含めて処理の分散が図られている場合については、業務サービス継続性の観点からは、国内以外であることの問題は特に生じないと考えられます。

(2) データ保護の観点から、要保護情報が含まれない場合、もしくは要保護情報を含む場合であっても要保護情報が利用者データ取扱サービスと同様に暗号化、もしくは匿名化された状態であれば、国内データセンタである必要はありません。

３．２　SaaS の検討

1) 業務系のクラウドサービス

災害時の安否確認システムや職員の業務管理システム等、業務系のクラウドサービスについては、IaaS/PaaS の利用者データ取扱サービスと同様に検討してください。

2)コミュニケーション系のクラウドサービス

メール・スケジュール管理等を中核とする統合コミュニケーションシステムやオンラインストレージ等、コミュニケーション系のクラウドサービスについては、IaaS/PaaS の利用者データ取扱サービスと同様に検討してください。

3)運用管理系のクラウドサービス

クラウドの利用が広まるに伴い、システムの運用監視、運用自動化、構成管理等の運用管理系のクラウドサービスの利用が増えています。

運用管理系のクラウドサービスについても、IaaS/PaaS の運用管理サービスと同様に検討してください。ただし、要保護情報の考え方については、運用管理系のクラウドサービスの性格から慎重な検討が必要になります。

特に、設計、設定、構成、資産などの情報への当該サービスによるアクセスが暗号化・匿名化なしに必要とされる場合については、サーバを設置するデータセンタが国内か国外ではなく、そのサービス全体のデータ保護対策を総合的に判断し、サービス利用のメリットとリスクを検討する必要があります。

また、運用管理系のシステムに、IaaS/PaaS などの管理対象システムへのアクセス用認証情報（アクセスキー、ID/パスワード、証明書等）を保持する場合、アクセス用認証情報に付与される権限が必要性に応じて最小であり、か

つ盗取や不正利用に対して十分な対策が取られていることを要します。

4)セキュリティ系のクラウドサービス

クラウドサービスの一つの形態として、セキュリティ系のサービスをクラウド化する動きが顕著となっています。EDR(Endpoint Detection and Response)、CASB(Cloud Access Security Broker)、SIG(Secure Internet Gateway)、SASE (Secure Access Service Edge)等のセキュリティ系クラウドサービスが該当します。また、従来からマネージド・セキュリティ・サービスとして外部サービス化されていたものも含みます。

セキュリティ系のクラウドサービスついては、基本的に、IaaS/PaaS の利用者データ取扱サービスと同様に検討してください。ただし、利用者データ、要保護情報の考え方については、セキュリティ系のクラウドサービスの性格から慎重な検討が必要になります。

利用者データを預け、その分析を依頼するクラウドサービスとなりますので、サーバを設置するデータセンタが国内か国外ではなく、利用する業務の性格に応じて慎重に検討する必要があります。

特に、以下のデータが監視・管理対象機器等から暗号化・匿名化されずにクラウドサービス側に転送される仕様であり、それがセキュリティ分析等、該当サービスの本来目的のために不可欠である場合、そのサービス全体のデータ保護対策を総合的に判断し、サービス利用のメリットとリスクを検討する必要があります。

(1) 利用者データ（利用者属性データ等）
(2) サービスの管理データやシステムデータ等（ネットワークのペイロード情報を含まないパケット情報、IP アドレス、ネットワークフローの挙動情報、クラウド利用アカウント ID の活動ログ、クラウドのシステム構成情報等）
(3) パスワードやクレデンシャル等に該当するデータ
(4) セキュリティ運用ポリシーを実行するためのデータ

４　クラウド基本方針や他の検討会との整合性

本文書については、今後、「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」（2018 年 6 月決定）や「クラウドサービスの安全性評価に関する検討会」等、クラウドに関する他の検討状況を確認しつつ、内容を整理していきます。