クラウドサービス利用ガイドライン　チェックリスト

記入年月日:　　年　月　日
記入者所属・氏名:　　・

チェックリストの使い方
1. チェック欄には、空欄:未確認　〇:確認した、基準をクリアしている　×:基準をクリアしていない　のいずれかを選択してください。
2. チェック内容メモ欄は、確認した内容の備忘録として利用してください(項目名が入っている欄は必ず記入してください)。
3. 情報の管理者への報告の際にご利用ください。
4. インシデントが発生した場合、利用状況等の確認のため提出を求められることがありますので、チェック後も大切に保管してください。
　あらかじめ担当部署に提出して保管を依頼することもできます。
5. クラウドサービスの類型によって、確認すべき項目が異なります。

サービス類型
〇:確認が必要な項目
△:注意が必要な項目(サービスの使い方によって確認が必要となる項目)

ガイドライン見出し	ガイドライン小見出し	ガイドライン	No.	〇は必須項目	チェック欄	ガイドラインチェック項目	チェック内容メモ欄	チェック欄	詳細チェック項目	サービス類型 SaaS	PaaS	IaaS
利用に向けた準備												
取り扱う情報の確認	情報の格付け	どの情報をクラウドサービス上に保存するのか(どの業務をクラウドサービスに移行するのか)を検討します。	1	〇		保存する情報の重要度は明確になっていますか？(別表1参照)	保存する情報:			〇	〇	〇
	クラウドサービスの選択	クラウドサービス利用基準に照らして、情報の重要度に応じたクラウドサービスを選択します。	2			クラウドサービス利用基準を満たしていますか？(別表2参照)	クラウド事業者名: クラウドサービス名:			〇	〇	〇
機関の組織・体制	クラウドサービス利用責任者	クラウドサービスの利用に関する責任者を決めます。責任者が不明だと、契約事項の確認やインシデント発生時の対応が難しくなります。	3	〇		クラウドサービスの利用について、機関側の責任者が明確になっていますか？	責任者所属: 責任者氏名:			〇	〇	〇
	クラウドサービス利用担当者	クラウドサービス事業者との窓口となる担当者を決めます。担当者は、クラウドサービス事業者との連絡のほか、ユーザアカウントの登録や削除、利用マニュアルの整備や指導、ヘルプデスクなどの業務を担当します。	4	〇		クラウドサービスの利用について、機関側の担当者を指名していますか？また担当者は、利用するクラウドサービスの機能について理解していますか？	担当者所属: 担当者氏名:			〇	〇	〇
機関の規則・契約	規則との整合性	機関のセキュリティポリシー、機関が保有する情報の取扱い規則、個人情報の取扱い規則などに準拠していることを確認します。情報の管理者が定められている場合は、クラウドサービス利用責任者は管理者に報告し、許可を得る必要があります。	5	〇		クラウドサービスを利用する機関の「情報セキュリティポリシー実施手順」を満たしていますか？				〇	〇	〇
			6	〇		機関が保有する情報の取扱い規則および個人情報の取扱い規則などを確認しましたか？				〇	〇	〇
			7	〇		情報の管理者にクラウドサービスを利用することを報告し、許可を得ましたか？				〇	〇	〇
	契約の取扱い	クラウドサービスの利用は業務の外部委託と同等です。契約の様式が異なっていても、機関の外部委託契約の基準に準拠している必要があります。個人情報や機密性の高い情報が含まれている場合、それぞれの取扱い規則との整合性の確認が必要です。約款に基づく契約の場合でも、これらに準じた取扱いが必要です。	8	〇		クラウド事業者との契約の内容は、機関の外部委託契約の基準を満たしていますか？				〇	〇	〇
			9	〇		個人情報や機密性の高い情報が含まれている場合、それぞれの取扱い規則との整合性を確認しましたか？				〇	〇	〇
利用範囲の明確化												
サービスの品質	SLA	クラウドサービスが安定して提供されないと利用者の業務遂行に支障をきたす恐れがあります。サービス停止の頻度や時間、応答時間などの性能、障害による停止時間や復旧時間が、利用を予定している業務の重要度に照らして許容できる範囲かどうかの検討が必要です。	10			サービス停止の頻度や時間、および性能などを確認しましたか？また、その内容は許容できますか？			クラウド事業者が保証している稼働率	×	〇	〇
									データ保証率	×	〇	〇
	メンテナンス	障害への対応やバージョンアップなどの定期メンテナンスによってサービスが停止する場合があります。特に定期メンテナンスは日時が指定できない場合があります。これらが利用者サービスに与える影響を評価し、許容できるかを検討します。	11			定期メンテナンスの頻度や時期が業務の妨げにならないことを確認しましたか？				×	〇	〇
	問い合わせ窓口・サポート体制	定期保守や障害時のクラウド事業者からの連絡方法および利用者からの問い合わせ窓口の確認が必要です。また利用者がサービスの状況を調べる方法や利用者向けの支援体制の有無と利用可能時間の確認が必要です。問い合わせや支援の依頼を利用者が個々に行うのか、担当者が取りまとめる必要があるのかの確認も必要です。	12			クラウド事業者からのサービスに関する連絡方法や状況の確認方法を確認しましたか？				〇	〇	〇
			13			問い合わせ窓口の有無、利用の方法、受付時間などを確認しましたか？			サービス提供時間帯(障害対応)	×	〇	〇
									サービス提供時間帯(一般問合せ)	△	〇	〇
	サービスの継続性	サービスが継続的に提供されるかどうかは、クラウドサービスに移行するかどうかを判断する上で非常に重要です。特にクラウド業者特有のサービスを使用する場合は、サービスの提供期間と契約終了後の代替手段の検討が必要です。	14			契約終了時の代替手段を検討しましたか？また、それは妥当ですか？				〇	〇	〇
機能とコスト	ネットワーク	サービスの利用に関してはクラウドサービス利用基準に準じていることが必要です。また担当者が管理を行う場合、管理業務を安全に行うことができるよう暗号化された通信路や適切なアクセス制御が行われていることを確認する必要があります。	15	〇		クラウドサービス利用担当者が使用する管理インターフェースの安全対策が行われていることを確認しましたか？			VPNを利用できるか	×	〇	〇
									ネットワークインターフェースが何個利用できるか	×	〇	〇
									ロードバランサを利用できるか	×	〇	〇
									F/Wが利用できるか	×	〇	〇
									通信の暗号化ができるか	〇	〇	〇
									リモート操作が利用できるか	×	〇	〇
									認証機能の種類	×	〇	〇
									グローバルIPを利用できるか	×	〇	〇
									IPアドレス制限ができるか	〇	〇	〇
									ネットワークトポロジを構築できるか(クラウド上に任意のネットワーク構成を構築できるか)	×	〇	〇
	管理ツール	利用者の管理、アクセス権の設定、メニューの選択など業務を行う上で必要な管理機能が提供されていることを確認します。一般的な機能であっても、明示されていない機能は提供されていない場合があります。	16			必要とする管理ツールの機能を満たしているか、または代替手段があるか確認しましたか？			稼働状況の一覧表示ツール	〇	〇	〇
									GUIベースで構成変更可能な管理ツール	〇	〇	〇
									負荷分散／フェイルオーバー機能の提供	×	〇	〇
									システムリソースの自動拡張・縮退	×	〇	〇
									ミドルウェアなどを設定済みのテンプレート	×	〇	〇
									互換クラウドの他社提供	×	〇	〇
									ログ監視・プロセス監視等	△	〇	〇
	ライセンス	機関が保有しているライセンスをクラウドサービス上で利用することが可能かどうか確認する必要があります。使用機材に紐付けられたライセンス、実環境と仮想環境で異なるライセンス体系を持つもの、クラウドサービス上での利用が許可されていないものなどがあります。	17			ライセンス数及びユーザ数は揃っていますか？CPUやコア数などを確認しましたか？				×	〇	〇
			18			クラウドを利用するシステムの開発ベンダに、ライセンス上問題がないことを確認しましたか？			想定するOSを利用できるか	×	〇	〇
									Oracle製品のライセンス(許可されてない場合が多い)	×	〇	〇
									保有しているOracleライセンスが利用できるか	×	〇	〇
									Microsoft製品のライセンス(許可されてない場合が多い)	×	〇	〇
	スケーラビリティ	リソース不足によるサービス低下を招くことがないよう、事前に必要な性能やデータ量などを検討しておく必要があります。また利用者数やデータ量の増加に対応できるか、その際の追加費用についても確認しておく必要があります。また時期によって負荷が大きく変動する業務への対応可能性についても確認する必要があります。	19			必要な性能やデータ転送速度を確認しましたか？			ネットワーク帯域は充分か	×	〇	〇
									レスポンス(応答時間)は問題ないか	×	〇	〇
			20			スケーリングの容易性やそれにかかる所要時間に問題ないか確認しましたか？			スペックレベル選択	×	〇	〇
									リソースの追加単位(CPU,メモリ,HDD)	×	〇	〇
			21			スケーリングの上限値を把握していますか？またそれに問題ないか確認しましたか？			グローバルIPの利用上限数	×	〇	〇
									作成可能な仮想数の上限数	×	〇	〇

ガイドライン見出し	ガイドライン小見出し	ガイドライン	No.	○は必須項目	チェック欄	ガイドラインチェック項目	チェック内容メモ欄	チェック欄	詳細チェック項目	サービス類型 SaaS	PaaS	IaaS
	利用料	平常時の費用だけでなく、現行システムからのデータ移行、カスタマイズにかかる費用などの一時的な費用、認証システムや既存のシステムとの連携のための費用などの追加的な費用が発生する場合があります。	22			クラウドサービスの利用料金、課金単位（時間ごと、日ごと、月ごとなど）および最低利用期間を確認しましたか？また、それは妥当ですか？				○	○	○
			23			他のシステムとの連携が必要な場合、その連携部分の構築・運用の費用を確認しましたか？				○	○	○
	回線使用料	回線使用料には、定額制のものと従量制のものがあります。不正アクセスなどの攻撃により通信量が急増する場合があるので、従量制を選択する場合には費用負担の考え方を確認しておく必要があります。	24			ネットワーク利用に必要なコスト、回線使用料は確認しましたか？また、それは妥当ですか？				×	○	○
	ストレージ	ストレージ価格に含まれる上限値の確認が必要です。高性能なストレージに大量のデータを保存するとかえってコストが高くなる場合があります。用途に応じたストレージを選択する必要があります。	25			ストレージの料金および追加料金を確認しましたか？また、それは妥当ですか？				○	○	○
クラウド事業者の選定												
データセンター	データセンターの場所	データセンターの場所を確認します。データセンターが海外の場合は、準拠法などの確認が必要です。サービスによっては場所が開示されない場合があります。	26			データセンターの所在地を確認しましたか？				×	○	○
	堅牢性	データセンターの物理的堅牢性を確認します。建物の耐震性、火災や水害への対策は重要です。また電源や空調の冗長性などについても確認します。	27			データセンターの安全設備を確認しましたか？また、それは妥当ですか？ データセンター基準 （http://www.jdcc.or.jp/pdf/facility.pdf）			ハザードマップ （http://disapotal.gsi.go.jp/index.html）	×	○	○
									防災対策	×	○	○
									防犯設備	×	○	○
	機密性	情報システムの機密性が高くても、設置場所の物理的な機密性が低ければ、その価値が大きく下がります。入館管理や監視体制などを確認します。	28			データセンターの運用体制を確認しましたか？また、それは妥当ですか？			入退室管理体制	×	○	○
									監視体制	×	○	○
									安全対策基準等に基づく認証の有無	×	○	○
クラウド事業者の信頼性	経営状況の確認	安定的なサービス提供がなければ、業務に支障をきたす可能性があります。クラウド事業者が他の事業者に買収された場合、これまでの同意事項が維持されず、セキュリティ要件に適合しなくなる場合があります。	29			適切なクラウド事業者を選定しましたか？			経営状況	○	○	○
									導入事例	○	○	○
									第三者認証の取得	○	○	○
	委託関係の確認	クラウド事業者は利用者との契約と異なる条件で第三者に外部委託したり、下請け契約を結んだりする場合があります。クラウド事業者が第三者のクラウドサービスを利用していることを明言していない場合、利用者がリスクを適切に評価できない場合があります。また第三者に委託していたクラウドサービスの終了などにより、サービスが継続できなくなったり、契約条件が変更されたりする場合があります。	30			クラウド事業者が第三者に業務を委託しているか確認しましたか？また、それは妥当ですか？				△	△	○
契約条件の確認												
責任範囲とペナルティ	責任範囲の明確化	障害発生時のクラウド事業者と利用者との責任分界点を確認しておく必要があります。クラウドサービスは多数の顧客に画一的なサービスを提供することで成り立っていることの理解が必要です。そのためサービス内容が少しずつ変更される可能性があります。変更に際する事前通知の有無や周知期間、不同意の場合の対応などをあらかじめ確認しておく必要があります。	31	○		利用者とクラウド事業者の責任範囲（責任分解点）は明確になっていますか？また、それは妥当ですか？				×	○	○
			32			契約期間中にクラウド事業者がクラウドサービスやSLAを変更する場合の手続き及び通知方法を確認しましたか？				○	○	○
	クラウド事業者のペナルティ	クラウド事業者側の過失でサービスの停止、データの喪失や情報漏えいなどが発生した場合の賠償の範囲や方法について確認が必要です。被害が甚大であっても、サービス停止・障害の間の料金の減額のみの保証であったり、明示的なペナルティ請求が必要であったりするため、契約条件の確認が必要です。	33			損害賠償、損失補償について契約で定めてありますか？また、それは妥当ですか？				○	○	○
データの所有権、返却・消去	データの所有権	クラウドサービスに保存したデータに対してクラウド事業者に所有権や利用権が発生する場合があります。	34	○		クラウドサービスに保存したデータの知的財産権，所有権及び利用権の取扱いを確認しましたか？また、それは妥当ですか？				○	○	○
	データの返却	契約解約時や終了時にデータが完全な形で返却されない場合があります。一つひとつのデータは取り出すことができても、まとまった形で取り出すことができない場合があります。他のクラウドサービスに移行する際、移行サービスが受けられない、あるいは多額の費用がかかる場合があります。	35			クラウドサービス利用中や契約終了時に，クラウドに保存したデータを取り出す方法があるか確認しましたか？				△	△	○
			36			契約終了時に，クラウド事業者から移行支援が受けられるか確認しましたか？				○	×	×
	データの消去	契約解約時や終了時にデータの消去を選択する場合、確実に消去されたことを確認できるか確認します。証明書を発行してもらうことができる場合があります。	37			契約終了時に，クラウド事業者が適正にバックアップを含むデータの消去を行ったことを確認する手段が提供されていますか？			データ削除	○	○	○
									削除証明書の発行	○	○	○
			38			契約終了時にアカウントの削除や再利用の禁止が可能であることを確認しましたか？			アカウント再利用	○	○	○
									アカウント削除	○	○	○
準拠法と管轄裁判所	準拠法	クラウドサービスに保存したデータは、サーバの設置場所の法律に準拠する場合があります。日本国内から利用していても、データ管理上の準拠法が異なる場合があります。また捜査機関がデータを差し押さえることを認めている国もあります。	39			準拠法を確認しましたか？また、それは妥当ですか？	準拠法：		データ保存場所（国や地域）	△	○	○
									準拠法の確認	○	○	○
	管轄裁判所	クラウド事業者によっては、本社の所在地を管轄裁判所としている場合があります。係争に発展した場合には多額の裁判費用がかかる場合があります。	40			管轄裁判所を確認しましたか？また、それは妥当ですか？	管轄裁判所：			○	○	○
運用体制の確認												
システムの運用に関する項目	セキュリティ対策	クラウド事業者側が運用する部分、機関側が運用する部分それぞれについて、セキュリティ対策が適切に行われているか確認します。機関側で疑似攻撃を伴う脆弱性のチェックを行う場合は、クラウド事業者に攻撃とみなされないよう注意が必要です。	41			バージョンアップ、設定変更、パッチ適用などのセキュリティ対策の方針を確認しましたか？			バージョンアップの頻度	△	△	○
									アップデート情報（脆弱性情報）報告の頻度	△	△	○
									ウイルス対策	△	△	○
	ログの監視	運用ログやセキュリティログが適切に保存されているか確認します。クラウドサービスの評価を行う際にも必要になります。クラウドサービス利用担当者がログを確認できない場合は、クラウド事業者から定期的に利用状況のレポートをもらうなど調整が必要な場合があります。	42			記録されるログの種類・期間を確認しましたか？				△	○	○
データの管理に関する項目	秘密鍵の管理	クラウドサービスを管理するための秘密鍵は非常に重要です。秘密鍵が紛失、破壊、漏えいしないよう厳重に管理する必要があります。また、クラウドサービスの利用者や利用担当者のパスワードの再発行手順についても確認が必要です。	43			パスワードの再発行等について、安全かつ適切な手順が提供されていますか？				○	○	○

ガイドライン見出し	ガイドライン小見出し	ガイドライン
	バックアップ	重要度が高いデータは消失に備えてバックアップが必要です。クラウドサービスに障害が発生していなくても、ネットワークの障害によってデータにアクセスできなくなる場合があります。
インシデントの管理に関する項目	インシデントの記録	クラウドサービス上で発生したインシデントについても機関内と同様に管理することが求められます。また機関側の責任でインシデントが発生した場合のペナルティについて確認しておく必要があります。

No.	○は必須項目	チェック欄	ガイドラインチェック項目	チェック内容メモ欄
44			情報の重要度やクラウドサービス内容に応じて、バックアップの取得方法、リストアの方法、保管方法などを決めましたか？	
45			クラウド事業者のデータの管理方法について確認しましたか？	
46			障害時の連絡方法を確認しましたか？	
47			障害やトラブル発生時の初期対応時の連絡先や連絡方法等を確認しましたか？	

チェック欄	詳細チェック項目	サービス類型 SaaS	PaaS	IaaS
	コピー及びイメージバックアップ	△	○	○
	自動及び手動バックアップ	△	○	○
	差分バックアップ	△	○	○
	バックアップ世代管理	△	○	○
	複数センターへの同時バックアップ	△	○	○
	指定場所バックアップ	△	○	○
	任意ダウンロード	△	○	○
	バックアップからのリストア	△	○	○
	任意な環境へのリストア	△	○	○
		○	○	○
		△	○	○
		△	○	○

別表1：機関が保有する情報の重要度

区分	情報格付け基準※との対応	区分の説明	情報の種類
重要度Ⅳ	3-2-2 3-2-1	情報が流出（漏えい）、紛失、改ざん等した場合、機関の業務に深刻かつ重大な影響を及ぼすもの	特定の関係者以外に対し厳重に機密を保持すべきもの
重要度Ⅲ	3-1-2 3-1-1 2-2-2 2-2-1	情報が流出（漏えい）、紛失、改ざん等した場合、機関の業務に重大な影響を及ぼすもの	特定の職制、グループ又は部局等以外に対して機密を保持すべきもの
重要度Ⅱ	2-1-2 2-1-1 1-2-2 1-2-1	情報が流出（漏えい）、紛失、改ざん等した場合、機関の業務に軽微な影響を及ぼすもの	公開を前提としていないもの（機関内限定）
重要度Ⅰ	1-1-2 1-1-1	情報が流出（漏えい）、紛失、改ざん等した場合、機関の業務にほとんど影響を及ぼさないもの	積極的な公開を前提としたもの

※「高等教育機関の情報セキュリティ対策のためのサンプル規程集」「B2104 情報格付け基準」

別表2：クラウドサービス利用基準