広島大学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　のど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. 文書管理者(グループリーダー，支援室長等)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。
   あらかじめ情報化推進グループに提出し，保管を依頼することもできます。

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	チェック内容メモ欄	ガイドラインチェック項目	チェック欄	詳細チェック項目
4. クラウドサービス利用範囲の明確化 4.1.利用前の確認	(1)クラウドサービス利用基準	・クラウドサービス導入前に，どの業務をクラウドサービスに移行するのか事前によく検討しましょう。 ・情報セキュリティインシデント発生時の影響の大きさなどを踏まえて，提供されているクラウドの情報セキュリティの水準を勘案し，クラウドサービスを使い分けることが必要です。	1	×の場合は要相談		クラウド事業者名: クラウドサービス名: 保存する法人文書:	・広島大学クラウドサービス利用基準をクリアしていますか？		
	(2)業務の継続性の保証	・クラウド業者固有のサービスを使用する場合は，そのサービスの継続性とサービス契約終了時の代替手段の検討が必要です。	2				・クラウドサービス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？		
4.2.信頼性	(1)SLA	・利用する業務の重要性に応じたサービスの停止や性能低下によるサービス低下などの許容範囲の検討が必要です。 ・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るので，障害による停止時間や復旧時間の目安の確認が必要です。	3				・サービス停止時間は確認しましたか？また，その内容は妥当ですか？		クラウド事業者が保証している稼働率
									データ保証率
	(2)メンテナンス	・クラウドサービスを利用しても故障と定期メンテナンスによりシステムが停止することがあります。特に，定期メンテナンスについては日時が調整できない場合があるので確認が必要です。	4				・定期メンテナンスが業務の差し障りにならないか確認しましたか？		
	(3)連絡方法・問い合わせ窓口	・クラウド事業者からの，計画停止予定通知等の方法の確認が必要です。	5				・連絡事項の通知，ウェブサイト掲載の有無を確認しましたか？		
		・クラウド事業者が対応可能な時間帯の確認が必要です。 ・クラウド事業者が直接利用者のサポート窓口を設置している場合や代理店等を経由する場合，又は本学の担当者が取りまとめてクラウド事業者に問い合わせする場合など，問い合わせの形態は様々です。	6				・サービス提供時間帯を確認しましたか？		サービス提供時間帯(障害対応)
									サービス提供時間帯(一般問合せ)
4.3.機能	(1)ネットワーク・通信	・【基準】利用者からデータ保存場所までの経路の暗号化　を満たしていることが必要です。 ・【基準】データのアクセス制限　を満たしていることが必要です。	7	〇			・クラウド管理担当者の利用する管理インターフェースが暗号化されているか確認しましたか？ ・アクセス制限の対象及び方法を確認しましたか？		VPNを利用できるか
									ネットワークインターフェースが何個利用できるか
									ロードバランサを利用できるか
									F/Wが利用できるか
									通信の暗号化ができるか
									リモート操作が利用できるか
									認証機能の種類
									グローバルIPを利用できるか
									IPアドレス制限ができるか
									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)
	(2)管理ツール	・クラウドサービスが有している機能が，必要な機能をきちんと満たしているか確認しましょう。 ・一般的な機能であってもメニューに掲載されていない機能は利用者に提供されていない場合があるので，必要な機能の有無の確認が必要です。	8				・必要とする管理ツールの機能を満たしているか，又は代替手段があるか確認しましたか？ ・必要なサービスの具体的な設定方法などは確認しましたか？		稼働状況の一覧表示ツール
									GUIベースで構成変更可能な管理ツール
									負荷分散／フェイルオーバー機能の提供
									システムリソースの自動拡張・縮退
									ミドルウェアなどを設定済みのテンプレート数
									互換クラウドの他社提供
									ログ監視・プロセス監視等
	(3)ライセンス	・本学が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時に，ライセンス契約に違反しないように注意が必要です。	9				・ライセンス数及びユーザ数は揃っていますか？		
		・仮想OS上でシステムが動作しても，ベンダがクラウド上への導入を許可していない場合があります。 ・特に，Oracleのデータベースライセンス等は，クラウド利用のための専用のライセンス以外はクラウド上で使うことが許可されていない場合があります。	10				・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か確認をしましたか？		想定するOSを利用できるか
									Oracle製品のライセンス (許可されてない場合が多い)
									保有しているOracleライセンスが利用できるか
									Microsoft製品のライセンス (許可されてない場合が多い)
	(4)スケーリング	・リソース不足によるサービス低下を招かないように，事前に必要な性能やデータ転送速度などを検討しておく必要があります。	11				・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
									レスポンス(応答時間)は問題ないか
		・クラウド利用の利点として，スケーリングが容易であると一般に言えますが，スケーリングが必要な業務の場合，スケーリングの容易性やその価格体系の確認が必要です。	12				・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
									リソースの追加単位(CPU,メモリ,HDD)
		・バースト(一時的な過負荷)が起こる業務の場合，対応可能か確認が必要です。	13				・スケーリングの限界を把握できていますか，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
									作成可能な仮想数の上限数

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	チェック内容メモ欄	ガイドラインチェック項目	チェック欄	詳細チェック項目
4.4.コスト	(1)利用料	・クラウドサービスを利用する際は，利用するシステム構成だけでなく，移行作業費・通信料・セキュリティ対策・バックアップ等総合的に費用の確認が必要です。 ・データベースライセンス等のライセンス料が高額になる場合があります。 ・APIが限定されていることによって，既存システムとの連携が複雑かつ高価になる場合があります。	14				・クラウドサービスの利用料金は妥当ですか？また，課金単位（日ごと，月ごとなど）及び最低利用期間を確認しましたか？		
	(2)ネットワーク	・回線使用料は，定額とデータ転送量に応じた従量課金があり，従量課金の場合は，上り下りで課金体系が異なる場合があるので，データ量に応じて課金されるかどうか確認が必要です。 ・VPN接続は別途追加料金が設定されている場合があります。 ・同一データセンター内にネットワークを構築する時に追加料金が発生する場合があるので確認が必要です。	15				・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？		
	(3)ストレージ	・大量のデータを保存する場合，ストレージのコストが高くなる場合があります。 ・特に，TB（テラバイト）以上のデータを扱う場合は，価格に見合うクラウドサービスか確認が必要です。	16				・ストレージの料金は確認しましたか？また，それは妥当ですか？		
4.5.データセンター	(1)物理的な対策	・データセンターの物理的な対策の確認が必要です。 ・クラウド事業者が，耐震性，冗長性，情報セキュリティなどの観点から安全性・信頼性の高いデータセンタを利用していないと，データの安全性が確保できません。	17				・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？		ハザードマップ（http://disapotal.gsi.go.jp/index.html）
									防犯設備
									入退室管理体制
									防災対策
									監視体制
5．本学の組織・体制	(1)クラウドサービス利用責任者	・本学の責任者が不明だと，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。	18	○		責任者所属： 責任者氏名：	・クラウドサービス利用について，本学の責任者が明確になっていますか？		
	(2)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が必要です。 【業務内容　例】 (1) ユーザアカウントの登録や抹消の処理 (2) 利用マニュアルの整備・指導 (3) ヘルプデスク (4) クラウド事業者との連絡調整	19	○		担当者所属： 担当者氏名：	・クラウドサービスの利用について，本学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特徴について理解していますか？		
6．本学の規則・契約	(1)本学の規則	・法人文書は，「法人文書管理規則」及び「個人情報の取扱いに関する規則」に沿って取り扱う必要があります。	20	○			・「法人文書管理規則」及び「個人情報の取扱いに関する規則」を確認しましたか？		
		・クラウドサービスを利用する情報は，クラウドサービス利用責任者から文書管理者（グループリーダー，支援室長等）に報告する必要があります。（平成25年4月の改正により，個人情報管理者は文書管理者と一緒になります。）	21	○			・文書管理者にクラウドサービスを利用することを報告しましたか？		
		・情報セキュリティポリシー実施手順で，重要度の高い情報の学外持ち出しを禁止している場合や，申請手続きが必要となっている場合があるので，確認しましょう。	22	○			・クラウドサービスを利用する組織の「情報セキュリティポリシー実施手順」と矛盾や不一致が生じないか確認しましたか？		
	(2)契約	・クラウドサービスの場合，Web上で約款が表示され，「同意します」ボタンをクリックするだけで，約款による契約が完了することがよくあります。（約款による契約とは，予め作成された契約の内容や条件を一律に定めた契約条項により契約を結ぶことを言います。） ※法人文書の重要度Ⅰの場合は約款による契約も可能ですが，この場合でも，書面による契約と同じ効力を持つので，「同意します」ボタンを押す前に約款をよく読んで本ガイドラインに沿っているかどうかチェックしましょう。	23				・法人文書の重要度Ⅱ以上の文書を保存する場合は，サービルを利用する時に契約書を取り交わしましたか？また，日本語での契約は可能ですか？		
		・クラウドサービスの利用は業務の外部委託と同等のものです。本学の契約書の様式で契約しない場合でも，「広島大学業務請負契約基準」に準じていることが必要です。 ・委託するデータに個人情報が含まれる場合，上記基準の「個人情報の取り扱い」の確認が必要です。 ・委託するデータに機密情報が含まれている場合，上記基準の「機密情報の取り扱い」の確認が必要です。	24	○			・クラウド事業者との契約の内容が，「広島大学業務請負契約基準」（https://commu.office.hiroshima-u.ac.jp/aqua/f7ccf08f-e6c3-4ad8-9799-d293ce2f68b4/view?exa=property）に準じていますか？		
7．クラウド事業者の信頼性	(1)クラウド事業者の選定	・クラウド事業者による安定的なクラウドサービス提供がなければ，業務に支障をきたす場合があります。 ・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できなくなる場合があります。	25				・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

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	チェック内容メモ欄	ガイドラインチェック項目	チェック欄	詳細チェック項目
	(2)第三者委託	・クラウド事業者は，利用者との契約と同じ保証を提供することができない第三者に外部委託したり，下請け契約を結ぶことができます。 ・クラウド事業者が本学の個人情報や機密保持を再委託先に渡す場合は，本学の承諾と本学の基準を遵守する義務を再委託先に負わせることを義務付けています。（「広島大学業務請負契約基準」の特記事項） ・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ければ，利用者がリスクを適切に評価できない場合があります。 ・クラウド事業者が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，諸条件が変更される場合があります。	26				・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？		
8．契約条件の確認	(1)責任範囲の明確化	・クラウド事業者と利用者の責任範囲が明確でないと，問題発生時に利用者が想定外の損害を被る場合があります。 ・障害発生時にクラウド事業者と利用者がどこまでの範囲で調査や対策を実施するのか確認が必要です。	27	○			・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？		
	(2)契約条件の確認	・クラウドサービスの変更に関して，通知期間，通知方法，不同意の場合の処理等が明確でなければ業務に支障をきたす場合があります。 ・クラウド事業者は，事前通知を行わないで，約款，SLA，価格，サービス内容の変更・停止等を行う場合があるので，事前通知の契約条件の確認が必要です。	28				・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？		
	(3)クラウド事業者のペナルティ	・クラウド事業者側の原因でデータ喪失したり，クラウドサービス障害により本学が波及損害を生じる場合があります。 ・クラウド事業者の過失により，情報漏洩，データ改竄，遵法違反等が発生する場合があります。 ・クラウド事業者の過失であっても，クラウドサービス停止・障害の間の料金が減額されなかったり，利用者が稼働レポートを確認し，必要に応じてペナルティ請求しなければ返金されない場合があるので，契約条件の確認が必要です。	29				・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，その内容は妥当ですか？		
	(4)準拠法	・クラウドサービスで保存しているデータは，サーバの設置されている国の法律に準拠するので，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。 ・国外の場合，調査機関がディスクを差し押さえて内容を見ることが認められている国があります。	30			データ保存場所：	・データ保存場所（国や地域）と，準拠法令を継続的に確認できますか？		データ保存場所（国や地域）
									パトリオット法の適用の有無
	(5)管轄裁判所	・クラウド事業者によっては，本社のある場所を「専属的合意管轄裁判所」としていることがあります。この場合，裁判のために海外まで弁護士を派遣したりすることになります。	31			管轄裁判所の所在地：	・管轄裁判所を確認しましたか？		
	(6)所有権	・契約条項で，クラウドサービスを利用して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しないことを確認する必要があります。	32	○（重要度Ｉ以外）			・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？		
	(7)データの確保	・利用者のデータが完全な形で返却されない場合があります。 ・クラウド事業者の突然の事業終了により，利用者が，データを取り出して他のシステムへ移行できなくなることがあります。	33				・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？		
	(8)契約終了時のデータの移行	・契約終了時に，データ移行作業支援が受けられない場合があります。	34				・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？		
	(9)契約終了時のデータの消去	・契約終了時の検討結果として，預けておいたデータを消去する必要が生じるかもしれませんので，この場合も考慮してデータを消去した証明書が提出できるかどうか確認する必要があります。	35				・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		データ削除
									削除証明書の発行
			36				・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		アカウント再利用
									アカウント削除
9．サービスレベル 9.1. システムの運用に関する項目	(1)セキュリティ対策	・クラウド事業者が管理するOS，アプリケーション，ハイパーバイザー等にセキュリティホールがあることで，情報セキュリティインシデントが発生する場合があります。 ・本学の情報セキュリティポリシー実施手順を基準にしたバージョンアップ方針の検討が必要な場合があります。 ・本学で，Webアプリコマンドのチェックやパッチ（OS，ミドルウェア，アプリケーションソフト等）を実施する必要がある場合があります。 ・本学で，ウイルス対策ソフトの利用と，定期的なウイルス検索の頻度の検討が必要な場合があります。 ・利用しているクラウドサービスに対して学内のサーバと同様に脆弱性のチェックを行う場合は事業者から攻撃ととられないよう注意が必要です。	37				・「バージョンアップ／変更管理／パッチ管理の方針」等のバージョンアップ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

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	チェック内容メモ欄	ガイドラインチェック項目	チェック欄	詳細チェック項目
9.2. データ管理に関する項目	(1)リソースの分離	・クラウド事業者の責任範囲内で不備があると以下のような問題が発生することがあります。 －利用者間でデータが漏洩してしまう。 －他の利用者の障害の影響が自社に及ぶ。 －利用者間のリソース分離の不備により，クラウドサービスの中断が発生する。 －利用者間のリソース分離の不備により，機密情報の漏洩が発生する。	38				・利用者ごとに適切に分離されているか確認しましたか？		
	(2)アクセス制限	・【基準】データのアクセス制限　を満たしている必要があります。 －重要度Ⅳ 担当者（決裁ラインにある上司も含め，業務を所掌する者）のみ －重要度Ⅲ 担当グループのみ －重要度Ⅱ 学内者のみ －重要度Ⅰ 公開用文書以外は，「学内者のみ」のアクセス制限を設けることが望ましい	39	○			・法人文書管理規則のアクセス制限が実現しているか確認しましたか？		
	(3)暗号化	・Unixの場合，Windowsのセーフモードのようにパスワードを忘れた時でもログインできるモードがないことが多いので，パスワード（秘密鍵）を紛失しないように注意が必要です。 ・秘密鍵は，SSL，ファイルの暗号化等を行うために重要なものです。秘密鍵の破壊や喪失は，セキュリティに重要な問題を生じる可能性があります。 ・クラウドサービスを利用する利用者やシステム管理者用のパスワードの再発行についても安全かつ適切な手順が必要です。	40				・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？		
	(4)ログ	・本学のクラウドサービス利用担当者やシステム管理者がログを見ることができないことがあるので，業務によってはログ確認の代替手段の検討が必要な場合があります。 ・運用ログやセキュリティログが適切に保存され，トラブルの際にログを参照できるようになっているか確認が必要な場合があります。 ・ログの喪失，改ざんに関する対策が必要な場合があります。 ・クラウド事業者に利用状況の統計を必要に応じてレポートしてもらい，クラウドサービスの評価を行うことが必要な場合があります。	41				・記録されるログの種類・期間を確認しましたか？		
	(5)バックアップ	・データ消失に備えてバックアップが必要です。 ・バックアップをデータセンターの外に置く場合は，ネットワークの帯域が影響して（特に，専用線を使っている場合）予定外に時間を要し，運用に適さない場合があります。この場合，差分バックアップにするなどの対策の検討が必要です。	42				・対象業務の重大性やクラウドサービス内容に応じて，バックアップデータの取得方法，保管方法等を決めましたか？ ・リストアの手順を確認しましたか？		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
		・データの重要度に応じてバックアップデータの管理方法等を確認しましょう。 ・バックアップデータからの漏えいやバックアップデータの消失等が発生することがあります。	43				・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？		
10. 情報セキュリティインシデントの管理		・クラウド事業者の責任範囲で発生した障害等を把握する方法を確認しておく必要があります。	44				・障害時の連絡方法を確認しましたか？		
		・本学の責任範囲でインシデントが発生した時の，クラウド事業者から本学へのペナルティを確認しておく必要があります。	45				・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？		