広島大学

クラウドサービス利用ガイドライン

2013 年 3 月 15 日策定

情報セキュリティ推進機構

修正履歴

2013 年 3 月 15 日　第一版

目次

１．目的 4
２．ガイドラインの位置付け 5
(1) 法人文書管理体制との関係 5
(2) ガイドラインの構成 6
(3) ガイドラインの見直し 6
３．クラウドサービス利用基準 7
(1) クラウドサービス利用基準 7
(2) クラウドサービスの独立性の高さ 8
(3) データのアクセス制限 9
(4) ネットワークの暗号化 9
(5) 今後検討を要する項目 9
４．クラウドサービス利用範囲の明確化 10
4.1.利用前の確認 10
(1) クラウドサービス利用基準 10
(2) 業務の継続性の保証 10
4.2.信頼性 10
(1) SLA 10
(2) メンテナンス 10
(3) 連絡方法・問い合わせ窓口 10
4.3.機能 11
(1) ネットワーク・通信 11
(2) 管理ツール 11
(3) ライセンス 11
(4) スケーリング 11
4.4.コスト 11
(1) 利用料 11
(2) ネットワーク 11
(3) ストレージ 12
4.5.データセンター 12
(1) 物理的な対策 12
５．本学の組織・体制 13
(1) クラウドサービス利用責任者 13
(2) クラウドサービス利用担当者 13
６．本学の規則・契約 14
(1) 本学の規則 14
(2) 契約 14
７．クラウド事業者の信頼性 15

(1) クラウド事業者の選定 15
(2) 第三者委託 15
８．契約条件の確認 16
(1) 責任範囲の明確化 16
(2) 契約条件の確認 16
(3) クラウド事業者のペナルティ 16
(4) 準拠法 16
(5) 管轄裁判所 16
(6) 所有権 16
(7) データの確保 17
(8) 契約終了時のデータの移行 17
(9) 契約終了時のデータの消去 17
９．サービスレベル 18
9.1. システムの運用に関する項目 18
(1) セキュリティ対策 18
9.2. データ管理に関する項目 18
(1) リソースの分離 18
(2) アクセス制限 18
(3) 暗号化 18
(4) ログ 19
(5) バックアップ 19
参考資料 21

１．目的

クラウドサービスは，サーバ管理の煩雑さを軽減し，新サービスの構築が迅速に行えることから注目を集めています。しかしその一方で，クラウドサービスはその運用の大部分がクラウド事業者の管理下で行われ，運用コストの最適化のため他の利用者とコンピュータ資源を共用する運用が行われるのが一般的です。そのため，データの保護・保全など情報セキュリティに関する懸念が指摘されています。

本学においても，管理運用業務の効率化の観点からクラウドサービスの積極的な活用が望まれますが，クラウドサービスの利用にあたっては，クラウド事業者の選定，サービス内容の確認，責任体制の構築等を慎重に行う必要があります。本学が保有している情報（法人文書）については，広島大学法人文書管理規則によりそれぞれの重要度に応じた取扱いが求められており，法人文書の保存場所としてクラウドサービスを利用する場合は特に慎重な対応が必要となります。

クラウドサービスを利用するには，クラウド事業者との間で外部委託契約を行うことになりますが，現時点ではクラウド事業者及び使用するサービス内容に対する基準等が定められていません。そこで，本学又は部局等が法人文書の保存場所としてクラウドサービスを利用する場合を想定した「広島大学クラウドサービス利用ガイドライン」（以下，ガイドラインという。）を策定しました。

本ガイドラインは，クラウドサービスの主な機能からその信頼度を定義し，法人文書の保存場所としてクラウドサービスを利用する際に，法人文書管理規則及び法人文書ファイル保存要領が定める重要度との対応関係を容易に確認できるようにするための補助資料です。したがって，本ガイドラインに拘束力はありませんが，クラウドサービスを利用する際に確認すべき項目が列挙されていることから，クラウドサービスの利用者は，**あらかじめ本ガイドラインのチェックリストにより確認することが望まれます。**また，今後クラウドサービスの利用においてインシデントが発生した場合には，**チェックリストによる確認結果について提出を求められる場合があります。**

２．ガイドラインの位置付け

(1) 法人文書管理体制との関係

本学の教職員が職務上作成し，又は取得した文書であって組織的に用いるものとして，本学が保有している文書は，紙媒体であっても電子媒体であってもすべて「法人文書」と呼ばれ，法人文書管理規則に沿って管理するべきものとなっています。法人文書の中には，学生指導に関する情報や，成績データなども含まれます。本学の法人文書は，その文書に含まれる情報が流出（漏えい），紛失，改ざん等した場合の影響の大きさで区分した重要度で分類されています（表 1）。

表 1．法人文書重要度分類表

区分		文書の種類	情報の類型（抜粋）
重要度Ⅳ	法人文書が流出(漏えい)，紛失，改ざん等した場合，本学の業務等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	○学籍簿，成績原簿に関する情報 ○指導要録の情報 ○医療に関する情報
重要度Ⅲ	法人文書が流出(漏えい)，紛失，改ざん等した場合，本学の業務等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	○学生指導に関する情報 ○卒業論文又は修士論文に関する情報 ○卒業後の就職・進路先情報
重要度Ⅱ	法人文書が流出(漏えい)，紛失，改ざん等した場合，本学の業務等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	○住所 ○氏名 ○生年月日 ○メールアドレス ○電話番号
重要度Ⅰ	法人文書が流出(漏えい)，紛失，改ざん等した場合，本学の業務等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	○公開講座等に関する情報 ○大学案内や広報誌に掲載している情報 ○募集要項に掲載している情報

重要度ごとに，紙文書に対しては施錠管理方法等が，電子文書に対してはアクセス権限が定めてあります。しかし，クラウドサービスでは保存場所の構築及び管理をクラウド事業者に委ねることになるため，クラウドサービスを利用して法人文書を保存する場合は，その妥当性を確認しておく必要があります。そのため，特にクラウドサービスを利用する場合の電子文書の保存場所・方法の基準としてガイドラインを策定しました（図 1）。

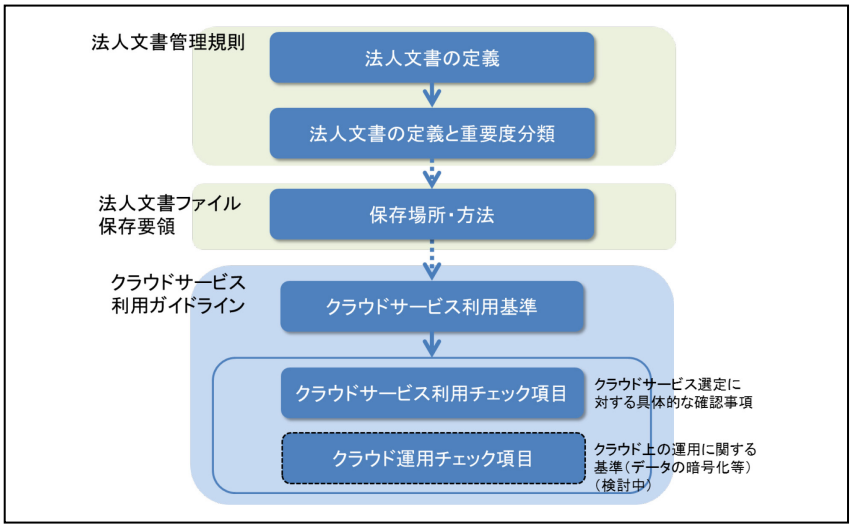

図 1．ガイドラインの位置付け

(2) ガイドラインの構成

３章のクラウドサービス利用基準では，クラウドサービスの信頼度を確認するための要件や，法人文書の重要度に応じて利用するクラウドサービスが満たしておいた方がよい要件を示しています。４章以降は，クラウドサービスの利用を決める前に知っておきたいリスクと，それを回避するために確認しておくべき内容の解説となっています。

別紙のチェックリストは，４章以降の解説に沿って比較的簡単にクラウドサービスの点検ができるものになっています（図 2)。このチェックリストは，大きく３つのパートに分かれています。まず，一番左は，本ガイドラインの４章以降の解説を記載してあります。また，その右に解説に対応した質問形式となっているガイドラインチェック項目と，チェックポイントである詳細チェック項目が並んでいます。

なお，利用予定のクラウドサービスの種類（IaaS,PaaS,SaaS など）によっては，チェック項目に関する情報がクラウド事業者から利用者に開示されていない事項や確認不要の事項などもあります。

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？		

図 2. チェックリスト

(3) ガイドラインの見直し

ガイドラインは，定期的（1 年程度）に点検を行う予定です。また，それ以外にも見直しを行うことがあります。

３．クラウドサービス利用基準

クラウドサービスとは，おおまかに言うと，キャンパスから離れたところに学内と同等の状態のネットワークやサーバを設置し，データを保存したり，アプリケーションを動かしたりすることです。そのため，学内にサーバを設置する時と比べて，① クラウド事業者が提供する資産を利用するので，１つのリソース（ハードウェア等）を他の組織と共有する可能性がある，② 学内限定などのアクセス制限ができない可能性がある，③ システム管理者がサーバにアクセスする時はインターネットを経由するので，サーバとシステム管理者データの通信が盗聴される可能性が高い，などいくつか異なる点があります。

(1) クラウドサービス利用基準

クラウドサービス利用基準（図 3）は，学内に設置したサーバとクラウドサービスの相違点を比較することでクラウドサービスの利用に際して満たすべき要件（図 4）を列挙し，それにクラウドサービスの機能を対応させることでクラウドサービスの信頼度を定義しています。

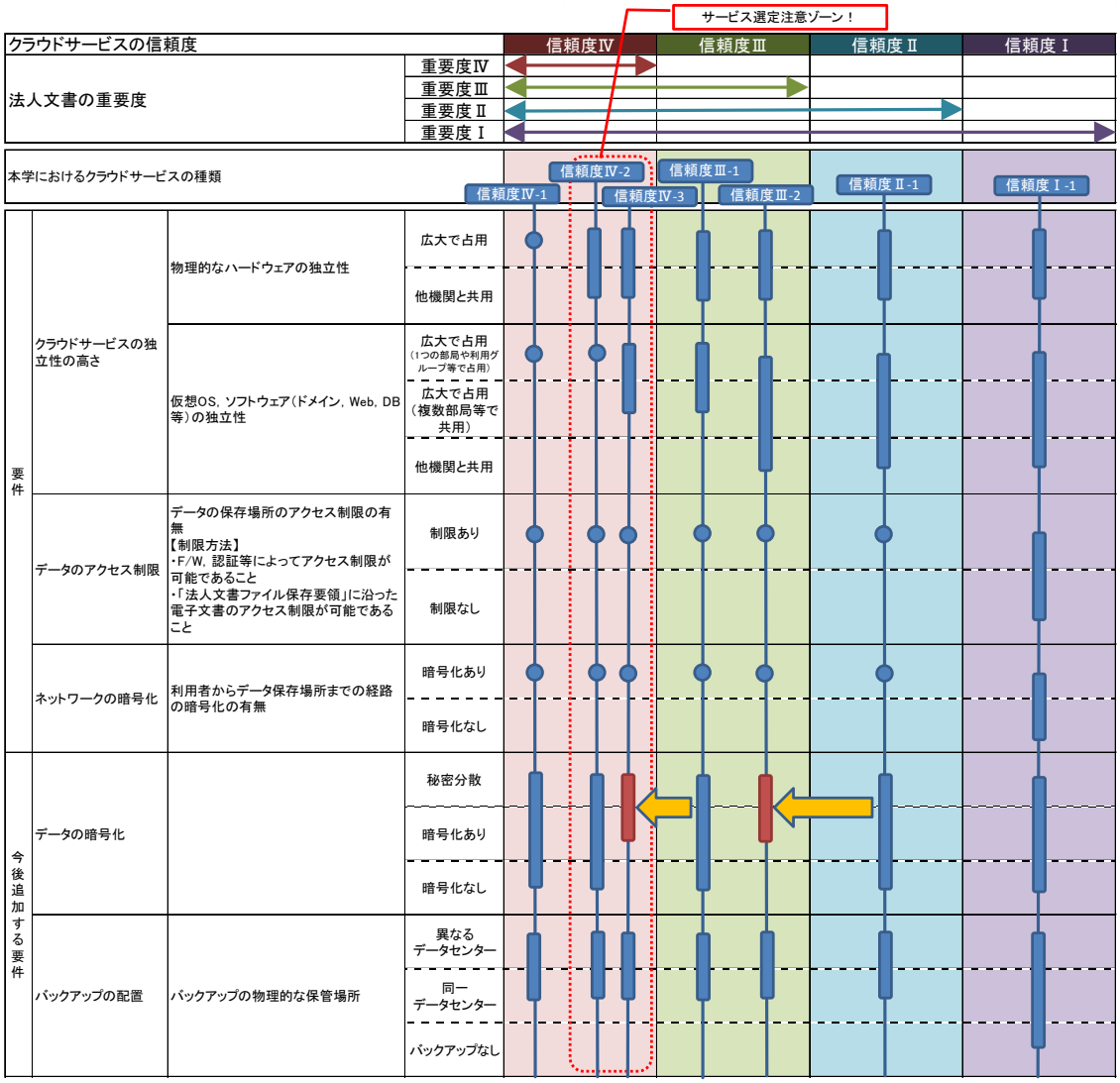

図 3．クラウドサービス利用基準

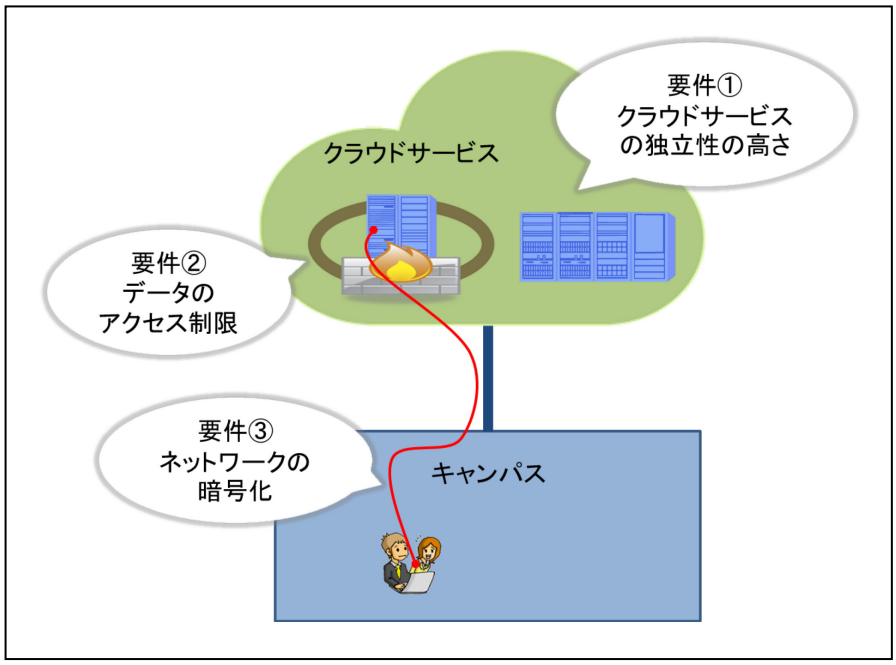

図 4. 満たすべき要件

(2) クラウドサービスの独立性の高さ

法人文書が学外に流出すると本学に大きな不利益となるので，重要度の高い法人文書は，厳密な施錠管理や業務担当者や担当グループに限定したアクセス制限が必要です。一方，クラウドサービスでは，1 つのハードウェアやシステムを複数の利用者（利用機関・組織・グループなど）で利用することがあり，このようなクラウドサービスを選択した場合，利用者間で情報が流出するリスクが高くなる可能性もあります。そのため，利用者間を隔離している度合いをクラウドサービスの信頼度の要件としています（図 5）。

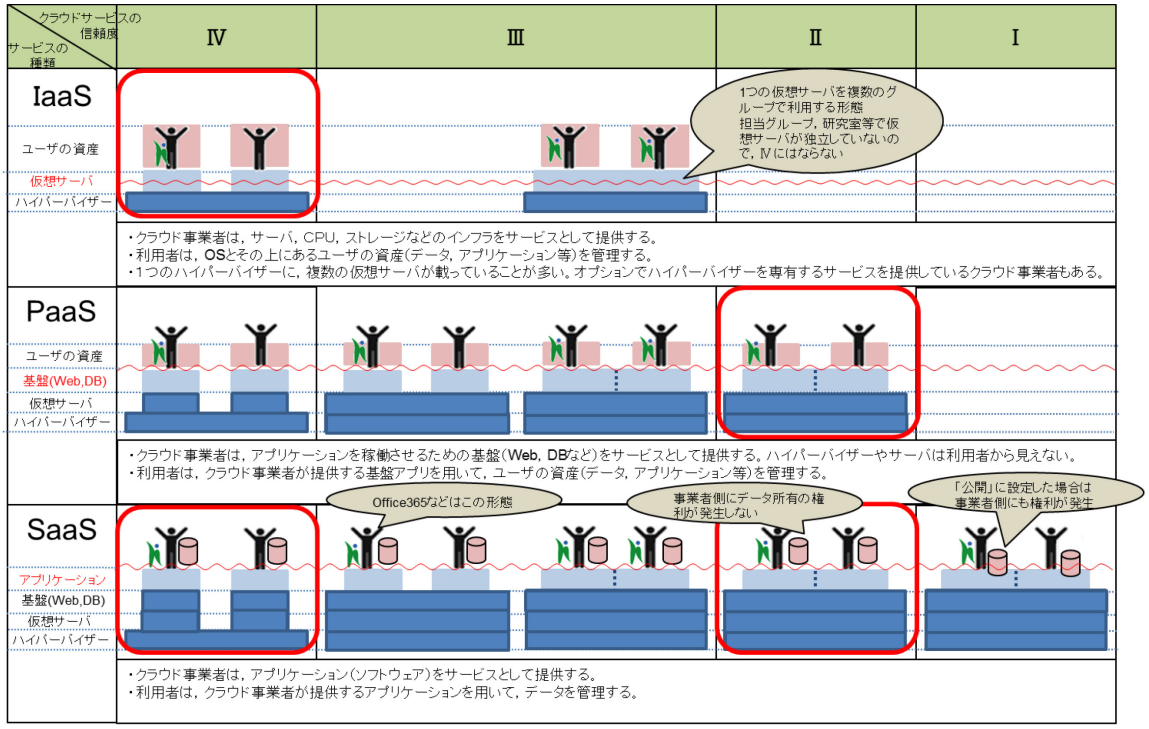

図 5. クラウドサービスの独立性の高さ

図の波線（赤）は，クラウド事業者と利用者の責任分解点を示しています。波線より下はクラウド事業者が責任を持って提供・保守している範囲です。この範囲が，より深い階層で分かれているほどクラウドサービスの独立性が高くなり信頼度が上がります。波線より上は，利用者の資産として，利用者の責任において準備・保守しますが，学内に設置したサーバと同じくセキュリティ等の管理が必要です。

(3) データのアクセス制限

キャンパスネットワーク（HINET2007）上に設置しているサーバは，設置しているゾーンによって学外からアクセスできないようにすることができます。また，サーバ管理者が，サーバごとに IP アドレス制限等を設定することがあります。しかし，クラウドサービスによっては，提供している機能の不足からこのようなアクセス制限ができない可能性があります。また，利用するアプリケーションによっては業務担当者ごとの詳細なアクセス制限などができなくなる可能性もあります。そのため，クラウドサービスの種類（IaaS, PaaS, SaaS など）に応じたデータへのアクセス制限機能が必要となります。

この要件に関しては，チェックリストで必要な機能等のチェックを行うことで確認してください。

(4) ネットワークの暗号化

クラウドサービスでは，システム管理者もインターネットを経由してサーバと通信を行うことがあります。インターネットを利用することで，データの通信が盗聴される可能性が高くなるので，利用者からデータ保存場所までの経路が暗号化できることが必要です。

(5) 今後検討を要する項目

データの秘匿性を向上させる技術として，暗号化技術があります。クラウド上に保存するデータを暗号化することにより，クラウドサービスの信頼度が向上すると考えられます。（P.7「クラウドサービス利用基準」の黄色矢印のとおり。）今後，暗号化の方法やアルゴリズムの選定等について検討を行います。

データの保存場所としてクラウドサービスを利用する場合，データの制御権を失わないように注意する必要があります。そのため，データが 1 ヶ所にしか存在しない状態を作らない(バックアップを作成する)こと が重要です。今後，サービスの選択やバックアップの作成方法についても検討を行います。

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

クラウドサービスの利用を決定する前に確認する事項をまとめています。

(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の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。

(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。

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。

(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。

(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。

・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。

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。

(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。

(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。

・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。

(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。

・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。

・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。

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。

(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。

(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。

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。

５．本学の組織・体制

クラウドサービスを利用する際の，本学の組織・体制について確認する事項をまとめています。

(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。

(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

６．本学の規則・契約

本学の規則及び契約手続きについて確認する事項をまとめています。

(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。

・法人文書の保存場所としてクラウドサービスを利用する時は，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。）

・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。

(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。

・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。

７．クラウド事業者の信頼性

クラウド事業者の信頼性について確認する事項をまとめています。

(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。

(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。

８．契約条件の確認

契約条件について確認する事項をまとめています。

(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。

(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。

(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。

(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。

(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。

(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。

(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。

(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。

(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。

９．サービスレベル

運用に入った後に確認する事項をまとめています。

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。

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。

(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。

(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。

(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。

(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。

・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。

10. 情報セキュリティインシデントの管理

情報セキュリティインシデントが発生した際の対応について確認する事項をまとめています。

・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。

・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。

参考資料

■Cloud Computing：Information Assurance Framework
クラウドコンピューティング：情報セキュリティ確保のためのフレームワーク
■Cloud Computing：Benefits,risk and recommendations for information security
クラウドコンピューティング：情報セキュリティに関わる利点，リスクおよび推奨事項
2009 年 11 月　ENISA: European Network and Information Security Agency
欧州 ネットワーク情報セキュリティ庁

■The NIST Definition of Cloud Computing
NIST によるクラウドコンピューティングの定義
2011 年 9 月　NIST：National Institute of Standards and Technology
米国国立標準技術研究所

■クラウドサービス利用のための情報セキュリティマネジメントガイドライン
2011 年 4 月 1 日　経済産業省

■中小企業のためのクラウドサービス安全利用の手引き
■クラウド事業者による情報開示の参照ガイド
2011 年 4 月　独立行政法人情報処理推進機構

■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（2010 年度版）
2011 年 3 月 31 日　国立情報学研究所

本件に関するお問い合わせ，ご意見等は以下までお願いいたします。
情報セキュリティ推進機構　　E-mail：sec-kikou@ml.hiroshima-u.ac.jp