広島大学

クラウドサービス利用ガイドライン

2017 年 8 月 7 日改訂

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

2015 年 9 月 1 日　第二版

2017 年 8 月 7 日　第三版

目次

１．はじめに

(1) 背景と目的

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。

(2) ガイドラインの取り扱い

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，**クラウドサービスを利用する場合は，導入前に本ガイドラインのチェックリストにより確認を行い，その結果を情報化推進グループ（下記）に提出してください。**

クラウドサービスは頻繁にそのサービス内容を変更しています。クラウドサービスの利用者は，利用中のサービスが利用当初のサービス内容が維持されているかどうかを定期的に確認する必要があります。**クラウドサービスの利用者は，１年を超えない期間ごとにその時点での最新のチェックリストにより確認を行い，その結果を情報化推進グループ（下記）に提出してください。**

なお，本学におけるクラウドサービスの利用状況の把握やインシデント対応等のため，**チェックリストの内容について説明を求められることがあります。**

［チェックリスト提出先］

財務・総務室情報部情報化推進グループ（総務担当）

E-mail：jyoho-soumu@office.hiroshima-u.ac.jp

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 ○住所 ○氏名 ○生年月日 ○電話番号
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	○学術講演会に関する情報 ○後援名義に関する情報 ○入試の実施計画に関する情報
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）。

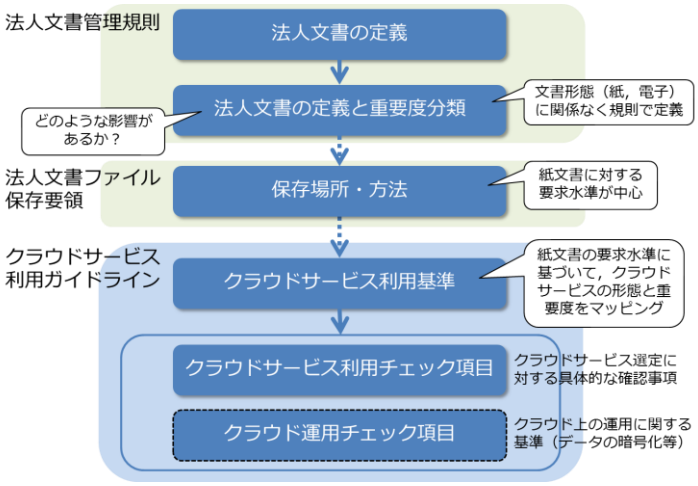

図 1. ガイドラインの位置付け

(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。

クラウドサービスの代表的な種類としては IaaS（Infrastructure as a Service），PaaS（Platform as a Service），SaaS（Software as a Service）などがあり，利用予定のものによっては，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。

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　○:確認した、基準をクリアしている　△:確認したが利用しない　×: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. 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. 1年を超えない期間ごとにチェックを行い、情報化推進グループに提出してください。
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
○: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	旧No.	No.	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
4. 利用に向けた準備(必須確認項目)												
4.1. 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	1		保存する情報の重要度は明確になっていますか？(ガイドライン表1参照)	保存する情報:			○	○	○
	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。	1,38,39	2		クラウドサービス利用基準を満たしていますか？(ガイドライン図3参照)	クラウド事業者名: クラウドサービス名:			○	○	○
4.2. 本学の組織・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。	18	3		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:			○	○	○
	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	19	4		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:			○	○	○

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。

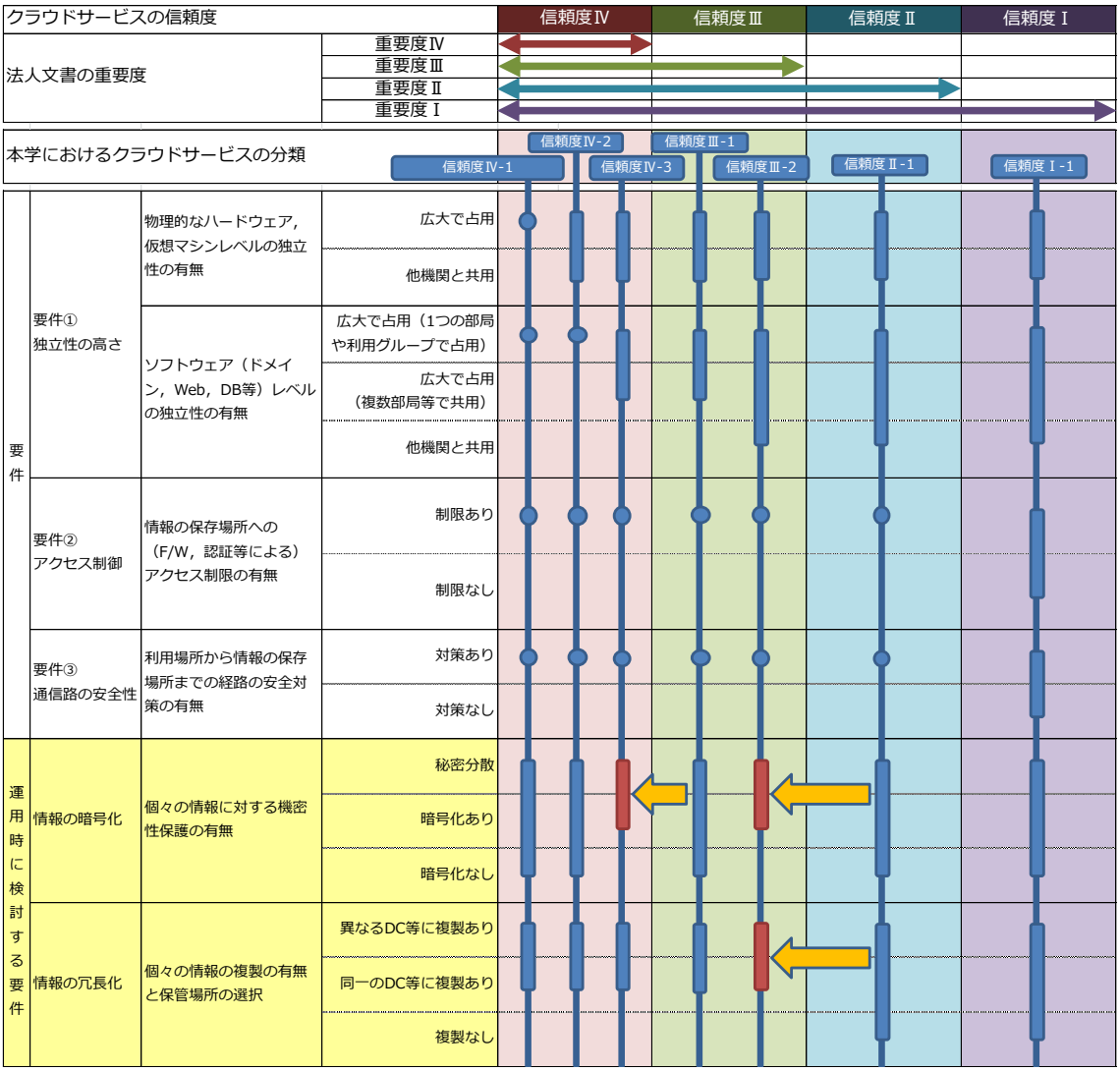

図 3. クラウドサービス利用基準

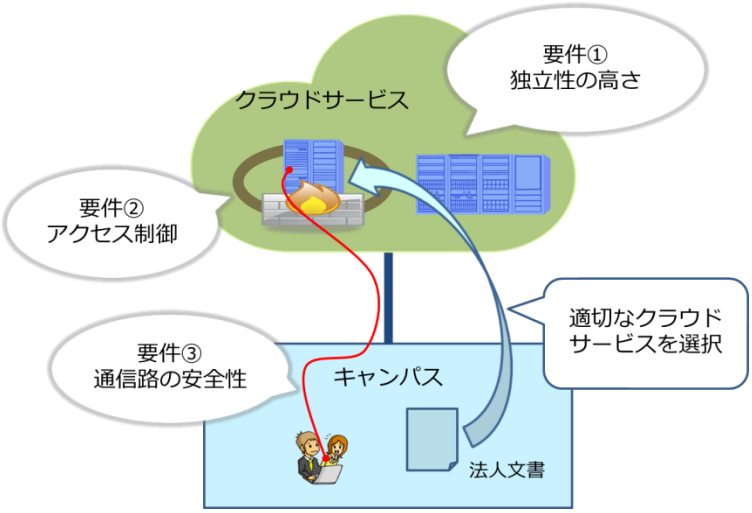

図 4. クラウドサービス利用基準の要件

(2) 要件①　独立性の高さ

クラウドサービスは，計算資源を仮想化技術によって複数の層（レイヤ）に分割し，それぞれのレイヤを責任分界点とするサービスモデルによって表現されます。クラウドサービスの種類（IaaS，PaaS，SaaS など）に応じて，クラウド事業者が提供するレイヤ（図 5 の薄青色部分）と責任分界ライン（図 5 の赤色波線）が決まります。

クラウドサービスを利用する時は，本学と他機関の利用者との間で共用されるレイヤと占用されるレイヤを確認し，責任分界ラインから下，つまり，クラウド事業者の責任範囲の“溝の深さ”によって独立性の高さを評価します（図 5～図 7）。また，責任分界ラインより上は，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。

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）で利用するため，サービスの独立性の高さ（隔離の度合い）でクラウドサービスの信頼度を評価します（図 8）。

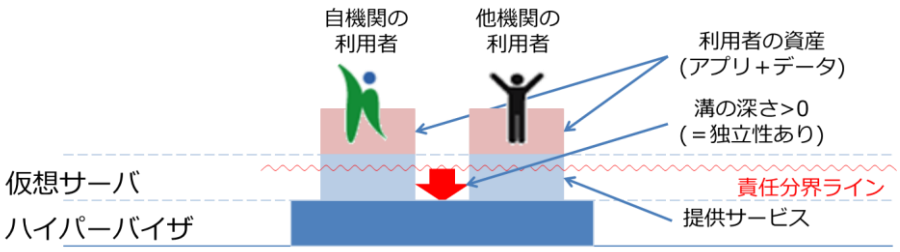

図 5. 独立性の高さ（IaaS の例）

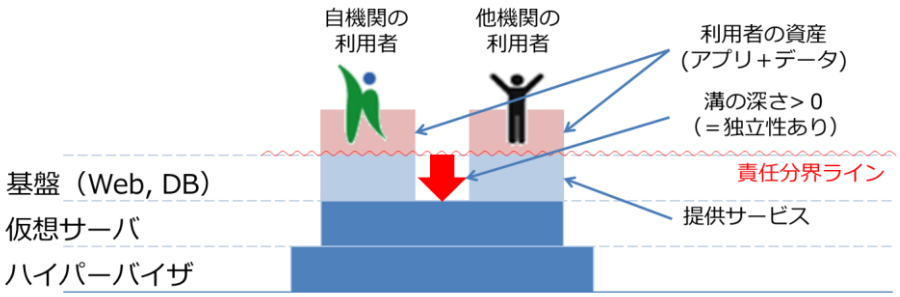

図 6. 独立性の高さ（PaaS の例）

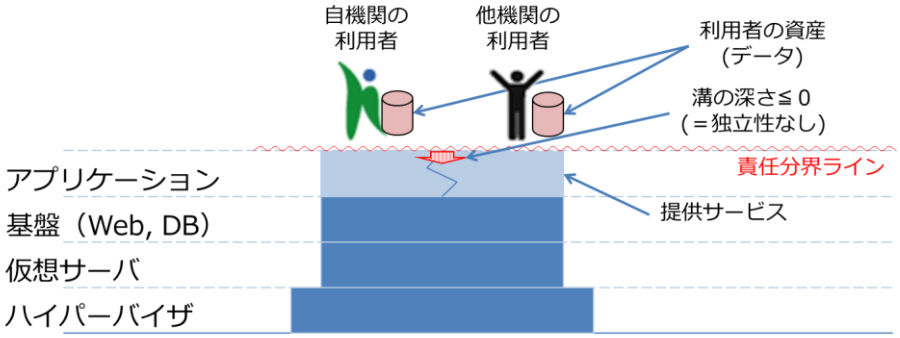

図 7. 独立性の高さ（SaaS の例）

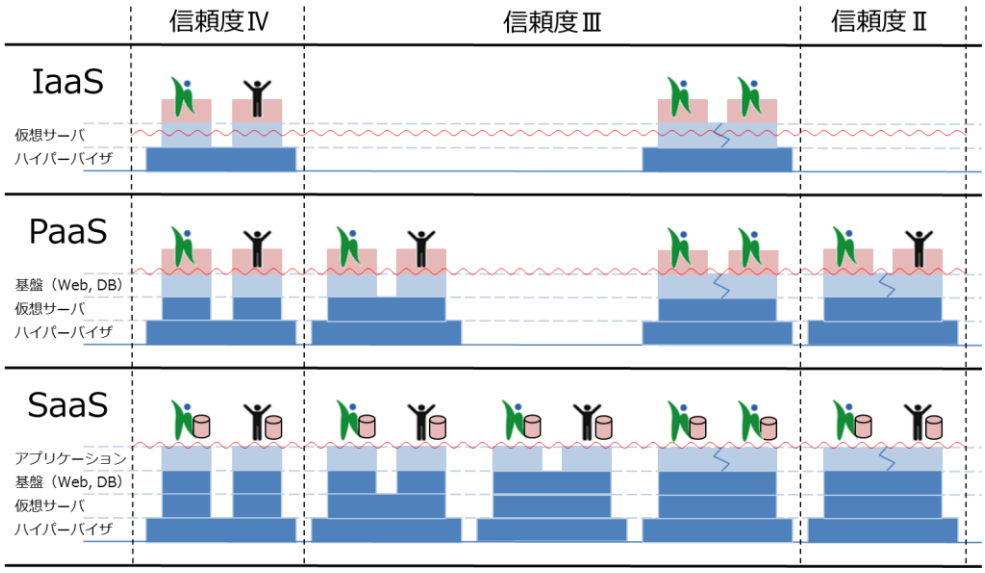

図 8. クラウドサービスの実装と信頼度の対応

(3) 要件②　アクセス制御

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，本学で管理しているサーバは，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，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求められていますが，利用するクラウドサービスの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。

(4) 要件③　通信路の安全性

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) 運用時に検討する要件

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（図 3 の黄色矢印)。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。サービスの選択やバックアップの作成方法について検討を行います。

４．利用に向けた準備

4.1. 取り扱う情報の確認

(1) 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。

(2) 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。

4.2. 本学の組織・体制

(1) 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。

(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。

4.3. 規則・契約

(1) 規則との整合性

「法人文書管理規則」，「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。法人文書の保管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。

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する必要があります。

(2) 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。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。特に，個人情報や機密情報が含まれている場合，上記基準の「個人情報の取り扱い」「機密情報の取り扱い」の確認が必要です。また，上記基準の特記事項で，クラウド事業者が個人情報や機密情報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。

５．利用範囲の明確化

5.1. サービスの品質

(1) SLA（Service Level Agreement）

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。

(2) 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保守によってサービスが停止する場合があります。特に定期保守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。

(3) 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。

(4) 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。特にクラウド事業者特有のサービスを利用する場合は，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。

5.2. 機能とコスト

(1) コンピューティング

利用するサービスが目的を実現できるものであるかどうか検討が必要です。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。

(2) 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。

(3) ネットワーク

必要な性能やデータ転送速度を検討しておく必要があります。

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。

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。

(4) 管理機能

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。

(5) ライセンス

本学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。

(6) コスト

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。

６．クラウド事業者の選定

6.1. データセンター

(1) 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。

(2) 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。

(3) 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。

6.2. クラウド事業者の信頼性

(1) 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。

(2) 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。

７．契約条件の確認

7.1. 責任範囲とペナルティ

(1) 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。

(2) 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洩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。

7.2. データの所有権，返却・消去

(1) 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。

(2) 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。

(3) 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。

7.3. 準拠法と管轄裁判所

(1) 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，データの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。

(2) 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。

８．運用体制の確認

8.1. 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。利用者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。

(2) 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。

8.2. データの管理に関する項目

(1) 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。

(2) 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。

8.3. インシデントの管理に関する項目

(1) 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学内と同様に管理することが求められます。また，利用者側の責任でインシデントが発生した場合のクラウド事業者から本学へのペナルティについて確認しておく必要があります。

参考資料

■NIST：National Institute of Standards and Technology（米国国立標準技術研究所）

- Guideline on Security and Privacy in Public Cloud Computing (SP-800-144)
  パブリッククラウドコンピューティングのセキュリティとプライバシーに関するガイドライン
  http://www.ipa.go.jp/files/000025365.pdf（日本語訳）
- Cloud Computing Synopsis and Recommendations (SP-800-146)
  クラウドコンピューティングの概要と推奨事項（SP-800-146）
  https://www.ipa.go.jp/files/000025367.pdf（日本語訳）

■ENISA: European Network and Information Security Agency
（欧州 ネットワーク情報セキュリティ庁）

- 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
  http://www.ipa.go.jp/security/publications/enisa/documents/Cloud%20Information%20Assurance%20Framework.pdf（日本語訳）
- 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
  http://www.ipa.go.jp/security/publications/enisa/documents/Cloud%20Computing%20Security%20Risk%20Assessment.pdf（日本語訳）

■経済産業省

- 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改訂版
- クラウドセキュリティガイドライン活用ガイドブック
  http://www.meti.go.jp/press/2013/03/20140314004/20140314004.html

■独立行政法人情報処理推進機構

- 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
  http://www.ipa.go.jp/security/cloud/tebiki_guide.html
- クラウドサービス安全利用のすすめ
  http://www.ipa.go.jp/security/cloud/cloud_tebiki_handbook_V1.pdf

■総務省

- クラウドサービス提供における情報セキュリティ対策ガイドライン
  ～利用者との接点と事業者間連携における実務のポイント～
  http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000073.html

■国立情報学研究所

- 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（2013 年度版）
  http://www.nii.ac.jp/csi/sp/

本文書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