富山大学
クラウドサービス利用ガイドライン

令和４年１月７日

情報委員会

改正履歴

版数	改正日	改正内容
第１版	令和４年１月７日	初版発行

目次

1. はじめに

1.1 目的

このガイドラインは,「国立大学法人富山大学におけるクラウドサービス利用要項」に基づき詳細な事項を定め，適切なクラウドサービスを利用することを目的とする。

1.2 対象

「国立大学法人富山大学学則」に定める教育研究組織等が運用主体となり，学内や学外に提供するサービスとしてクラウドサービスを利用する場合を対象とする。

1.3 定義

（1） クラウドサービス　インターネットを通じてソフトウェアやハードウェアを利用する情報システムサービスの総称。当ガイドラインでは，SaaS（Office365，Google Apps，Amazon AWS の一部サービス，iCloud，Dropbox 等），PaaS（Amazon AWS，Microsoft Azure の一部サービス等），IaaS（Amazon AWS，Microsoft Azure の一部サービス等）全てを指す。

（2） 情報機器　業務に関連する情報を取り扱うパソコン，タブレット，スマートフォン等の全ての機器

（3） ISMAP　政府情報システムのためのセキュリティ評価制度

1.4 ガイドラインの取り扱い

本ガイドラインは，クラウドサービスを利用する際に留意すべき内容が記載されています。

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を一読し，クラウドサービス利用申請書及びクラウドサービス利用事前確認チェックリスト（以下，チェックリストという。）を情報セキュリティ統括責任者（以下,「CISO」という。）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。そのため，クラウドサービスの利用責任者は，サービス内容及び契約条件等に変更がないかをチェックリストにて定期的に確認し，変更があった場合は，速やかに申請してください。変更がない場合であっても，毎年度継続のための申請が必要です。

なお，本学におけるクラウドサービスの利用状況の把握，情報セキュリティ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報告を求めることがあります。

2. ガイドラインの位置付け

2.1 情報の格付け及び取扱制限に関する規則との関連性

本学では，「国立大学法人富山大学における情報の格付け及び取扱制限に関する規則」並びに「国立大学法人富山大学情報格付け取扱手順」が制定されており，表 1-1～1-3 のとおり，取り扱う情報に明示等された格付け及び取扱制限に従い，情報を取り扱う必要があります。また，取り扱う情報，処理に関して，法令，「国立大学法人富山大学個人情報保護方針」並びに「国立大学法人富山大学個人情報保護規則」等の学内規則及び関連する学会のガイドライン等に違反していないか確認します。

表 1-1　格付け区分及び分類の基準

格付け区分	分類の基準
機密度３情報 （秘情報）	秘密保全の必要が高く，その漏えいにより，本学の信用を損ない，又は利益を害するおそれのある情報
機密度２情報 （関係者外秘情報）	機密度３情報に相当しないが，その漏えいにより，本学の活動の遂行に支障を及ぼすおそれのある情報
機密度１情報 （公開情報等）	公表済みの情報，公表しても差し支えない情報，機密度２情報又は機密度３情報以外の情報

表 1-2　取扱制限の種類及び指定例

取扱制限の種類	取扱制限（指定例）
複製	複製禁止，複製要許可
配付	配付禁止，配付要許可
暗号化	暗号化必須，保存時暗号化必須，通信時暗号化必須
印刷	印刷禁止，印刷要許可
転送	転送禁止，転送要許可
転記	転記禁止，転記要許可
再利用	再利用禁止，再利用要許可
送信	送信禁止，送信要許可
参照者の制限	関係者限り

表 1-3　情報の種類に基づく分類

機密度区分	対象情報	左記情報を含む可能性がある情報資産	取扱制限等
機密度３情報 （秘情報）	人種、世系又は民族的若しくは種族的出身	・戸籍謄本 ・戸籍抄本	暗号化必須 参照者の制限必須 （指定例） ・マイナンバー担当者限り ・謝金担当者限り ・問題作成担当者限
	信条（個人の基本的なものの見方、考え方（思想と信仰の双方を含む））	・相談記録	
	社会的身分（ある個人に境遇として固着していて、一生の間、自ら	・戸籍謄本 ・戸籍抄本	

	の力によって容易にそれから脱し得ないような地位)		り ・入試担当者限り 施錠保管必須
	病気に罹患した経歴	・患者診療情報 ・医師の診断書 ・健康診断記録 ・保健管理センター来所記録	
	犯罪の経歴（前科（有罪の判決を受けこれが確定した事実））	・懲戒処分に係る記録	
	犯罪被害事実（身体的被害、精神的被害及び金銭的被害の別を問わず、犯罪の被害を受けた事実)	・ハラスメント相談記録	
	心身の機能の障害（身体的障害、知的障害、精神障害（発達障害を含む）、特殊な疾病による障害があることを特定させる情報	・身体障害者手帳 ・療育手帳 ・医師の診断書 ・障害を有する学生に関する記録 ・受験配慮申請	
	健康診断等の結果	・健康診断記録 ・被ばく記録	
	保健指導、診療・調剤情報		
	本人を被疑者又は被告人とする刑事事件に関する手続		
	本人を非行少年等とする少年の保護事件手続		
	マイナンバー（個人番号）情報	・給与支払報告書 ・源泉徴収票 ・個人番号に関する報告書 ・謝金支給対象者名簿	
	作成中又は未実施の入試問題(解答及び解答に係る情報を含む)		
	合否判定前の入試成績情報	・入学試験成績一覧表 ・大学入試センター提供成績	
	合格発表前の入試合否情報	・合格者受験番号表 ・合格通知書 ・選抜結果通知書	
	学生及び職員等の事件・事故に関する情報	・懲戒処分に関する記録 ・ハラスメント相談記録	

		・不正行為に関する記録 ・事件・事故に関する報告	
機密度２情報 （関係者外秘情報）	機密度３情報,機密度１情報以外の情報	・個人情報を含む情報	暗号化必須 参照者の制限必須 （指定例） ・業務関係者限り
	・学内会議，各種委員会の資料	参照者の制限 （指定例） ・構成員限り ・構成員，陪席者限り	
	・その他	参照者の制限 （指定例） ・業務関係者限り	
機密度１情報 （公開情報等）	公表済みの情報,公表しても差し支えない情報	・大学案内 ・ウェブサイト掲載情報 ・パンフレット ・その他広報資料 ・学会等発表済研究論文 ・プレゼン資料 ・法律等により公開を義務付けられている情報	

2.2　ガイドラインの構成

「3. クラウドサービス利用基準」では利用するクラウドサービスが満たすべき要件を示しています。チェックリストにより，クラウドサービスの点検ができるものになっています。

2.3　ガイドラインの見直し

本ガイドラインは，随時見直しを行い，必要に応じて改訂を行います。

利用しているクラウドサービスが本ガイドラインに適合しなくなった場合，利用責任者は可及的速やかに，サービス継続について検討し，継続が必要であると判断した場合は，適合するクラウドサービスへ移行してください。

3. クラウドサービス利用基準

3.1 クラウドサービス利用基準

利用するクラウドサービスは，ISMAP に登録されているクラウドサービス事業者が提供するものであること，かつデータの保存場所がすべて日本国内であることを基準とします。

ただし，以下のものについては，CISO の承認があれば利用可能とします。

（1） ISMAP に登録されているが，データの保存場所が日本国外のもの

（2） ISMAP に登録されているが，データの通信経路が日本国外を経由するもの

（3） ISMAP に登録されていないもの

利用するクラウドサービスの ISMAP 登録状況，データ保存場所，準拠法及び裁判管轄に関する情報等については，ISMAP ポータル（https://www.ismap.go.jp/csm）から確認できます。

3.2 既に利用しているクラウドサービス

「国立大学法人富山大学におけるクラウドサービス利用要項」施行以前から利用のクラウドサービスについては，必要に応じて一定期間の利用を認めますが，「3.1 クラウドサービス利用基準」を満たすクラウドサービスに移行してください。

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。また，取り扱う情報，処理に関して，法令，学内規則及び関連する学会のガイドライン等に違反していないか確認します。

（2） クラウドサービスの選択

「2.1 情報の格付け及び取扱制限に関する規則との関連性」に照らして，情報の機密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） 利用責任者

利用するクラウドサービスに関する本学の責任者を決定します。なお，利用責任者は，「国立大学法人富山大学学則」に定める教育研究組織等の長，「国立大学法人富山大学事務組織規則」第 2 条及び第 3 条に定める事務局並びに事務部の課長等が該当します。

（2） 窓口担当者

クラウドサービス事業者との連絡，ユーザアカウントの管理，利用マニュアルの整備及びヘルプデスク等の業務を担当する者を決定します。

4.3 規則・契約

クラウドサービスでは，本学が管理していない学外の環境を利用し，その環境上でデータ管理，運用並びにアプリケーションを利用します。そのため，規則・契約において，学内ネットワークを利用して学内にサーバを設置するときと比較して，情報セキュリティの観点から留意すべき点が多く存在します。

5. 利用範囲の明確化

5.1 クラウドサービスの品質

（1） SLA（Service Level Agreement）

クラウドサービスが安定して提供されない場合，利用者の業務遂行に支障をきたす恐れがあります。クラウドサービスの停止頻度，時間及び応答時間等の性能，障害による停止期間及び復旧時間が，利用を予定している業務の重要度に照らして，許容できる範囲内か検討が必要です。

（2） メンテナンス

障害への対応やバージョンアップ等の定期保守によってクラウドサービスが停止する場合があります。これらが利用者に与える影響を評価し，許容できる範囲内かを検討します。

（3） 問い合わせ窓口・サポート体制

定期保守及び障害時のクラウドサービス事業者からの連絡方法及び利用者からの問い合わせ窓口の確認が必要です。また，窓口担当者がサービスの運用状況を調べる方法や利用者向けの支援体制の有無及び利用可能時間の確認が必要です。問い合わせ及び支援の依頼を利用者が個々に行うのか，窓口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） クラウドサービスの継続性

クラウドサービスが継続的に提供されるかどうかは，クラウドサービスへの移行を検討する上で非常に重要です。特にクラウドサービス事業者特有のクラウドサービスを利用する場合は，クラウドサービスの提供期間及び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

利用するクラウド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

必要な性能及びデータ転送速度を検討しておく必要があります。

管理業務を安全に行うことが出来るよう暗号化された通信路及び適切なアクセス制御が行われていることを確認し，接続先を確認した暗号化通信を行う必要があります。

回線使用料には，定額制のもの従量制のものがあります。不正アクセス等の攻撃により通信量が急増する場合があるため，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，アクセス権の設定及びメニューの選択等，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利用する場合，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。使用機材に紐づ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又はクラウドサービス上での利用を許可されていないもの等があります。

（６）　コスト

平常時の費用だけではなく，現行システムからのデータ移行，カスタマイズに係る費用又は認証システム及び既存システムとの連携のための費用等，追加的な費用が発生する場合があります。

（７）　認証

利用するクラウドサービスは，Azure Active Directory 認証もしくは Shibboleth 認証に対応しており，多要素認証の設定が可能なクラウドサービスを選択してください。

6. クラウドサービス事業者の選定

6.1 データの保存場所

（1） 場所

データの保存場所及び通信経路を確認します。データの保存場所及び通信経路がすべて日本国内である必要があります。クラウド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ので，注意が必要です。

（2） 堅牢性

データの保存場所の物理的堅牢性を確認します。建物の耐震性，火災及び水害への対策は重要です。また，電源及び空調の冗長性等についても確認します。

（3） 機密性

データの保存場所の物理的な機密性が低ければ，その価値は大きく下がります。入館管理及び監視体制等を確認します。

6.2 クラウドサービス事業者の信頼性

（1） 経営状況の確認

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可能性があります。クラウドサービス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

クラウドサービス事業者は，利用者との契約と異なる条件で第三者に外部委託する場合又は下請契約を締結している場合があります。クラウドサービス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等により，サービスが継続できなくなる場合又は契約条件が変更される場合があります。

7. 契約条件の確認

7.1 責任範囲と過失

（1） 責任範囲の明確化

障害発生時のクラウドサービス事業者と利用者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クラウドサービスを提供することで成り立っていることへの理解が必要です。そのため，クラウドサービスの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，周知期間又は不同意の場合の対応等をあらかじめ確認しておく必要があります。

（2） クラウドサービス事業者側の過失

クラウドサービス事業者側の過失でクラウドサービスの停止，データの喪失又は情報漏洩等が発生した場合の賠償の範囲及び方法についての確認が必要です。被害が甚大であってもクラウドサービスの停止及び障害の間の料金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，返却及び消去

（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，クラウドサービス事業者側に所有権又は利用権が発生する場合があります。

（2） データの返却

契約解約時又は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。1 つ 1 つのデータを取り出すことはできても，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，又は多額の費用がかかる場合があります。

（3） データの消去

契約解約時又は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します。証明書等の書面で提供されることが望ましいです。

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されたデータは，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。利用するクラウドサービスは，締結する契約に定める準拠法が日本法である必要があります。

（2） 管轄裁判所

クラウドサービス事業者によっては，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，多額の裁判費用が掛かる場合があります。利用するクラウドサービスは，所轄裁判所を日本国内の裁判所である必要があります。

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

クラウドサービス事業者側が運用する部分，本学側が運用する部分について，セキュリティ対策が適切に行われているか確認します。また，クラウドサービス上に保存する情報については，情報の機密度に応じて暗号化を行います。

（2） ログの監視

運用ログ及びセキュリティログが適切に保存されているかを確認します。クラウドサービスの評価を行う際にも必要になります。ログを確認できない場合は，クラウドサービス事業者から定期的に利用状況の報告を貰う等の調整を行う必要があります。

8.2 データ管理に関する項目

（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（暗号化されたものを復号する鍵）は重要です。秘密鍵を紛失，破損及び漏洩しないよう，厳重に管理する必要があります。また，利用者のパスワード再発行の手順についても確認が必要です。

（2） バックアップ

重要度の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出来なくなる場合があります。

8.3 インシデント管理に関する項目

（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，学内で発生したインシデントと同様に対応する必要があります。契約時には，本学側とクラウドサービス事業者側が負うべき責任範囲を明らかにします。

情報セキュリティインシデント発生時，利用責任者は，データの保全に努め，状況確認等の調査に協力することとします。なお，この場合のクラウドサービス事業者から本学への責任範囲についても確認しておく必要があります。

9. その他

「国立大学法人富山大学におけるクラウドサービス利用要項」に違反した場合，又は本学の情報セキュリティが著しく損なわれると判断される場合，CISO は，クラウドサービスの利用を強制的に停止できるものとします。