サンプル規程集対応チェックリストVer.1.0

【解説】

国立情報学研究所の「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（2019 年度版）」では、
大学・研究機関でセキュリティポリシやクラウドサービス利用時のガイドラインを策定する際に検討すべきことを例示しています。
https://www.nii.ac.jp/service/sp/

学認クラウド導入支援サービスでは、大学・研究機関がクラウドを導入する場合の着眼点(信頼性、セキュリティ、契約条件等)を
まとめたクラウドチェックリストを策定し、公開しています。
https://cloud.gakunin.jp/foracademy/#academy-02

本資料は、
国立情報学研究所の「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（2019 年度版）」のうち、
具体的なセキュリティ対策規程のサンプルが記載されている「D2101 情報セキュリティ対策基準」(以下「サンプル規程集」)、
および「学認クラウド導入支援サービスクラウドチェックリストVer.5.0」(以下「クラウドチェックリスト」)に基づいて、
大学・研究機関でパブリッククラウドサービスを利用する場合の情報セキュリティに関するチェックポイントをまとめたもの
です。

具体的には、
- サンプル規程集の条文のうち、パブリッククラウド利用に関係する記述に関して、対応するクラウドチェックリストの項目を
  抽出しました。
- また、抽出したクラウドチェックリストの各項目に対して、サンプル規程集で規定した要件を満たすために有効であると
  考えられるベストプラクティスを記載しました。

「項目順セキュリティサンプル規程集対応チェックリスト」には、抽出したクラウドチェックリストの項目が項番順に、ベストプラクティスと
それを満たすためのチェックリスト回答とともに記載されています。また、情報の機密性・完全性・可用性との関連が「〇」で示されて
います。

「条文順セキュリティサンプル規程集対応チェックリスト」には、サンプル規程集の条文が条文順に、対応するクラウドチェックリストの
項目、ベストプラクティスとそれを満たすためのチェックリスト回答、とともに記載されています。

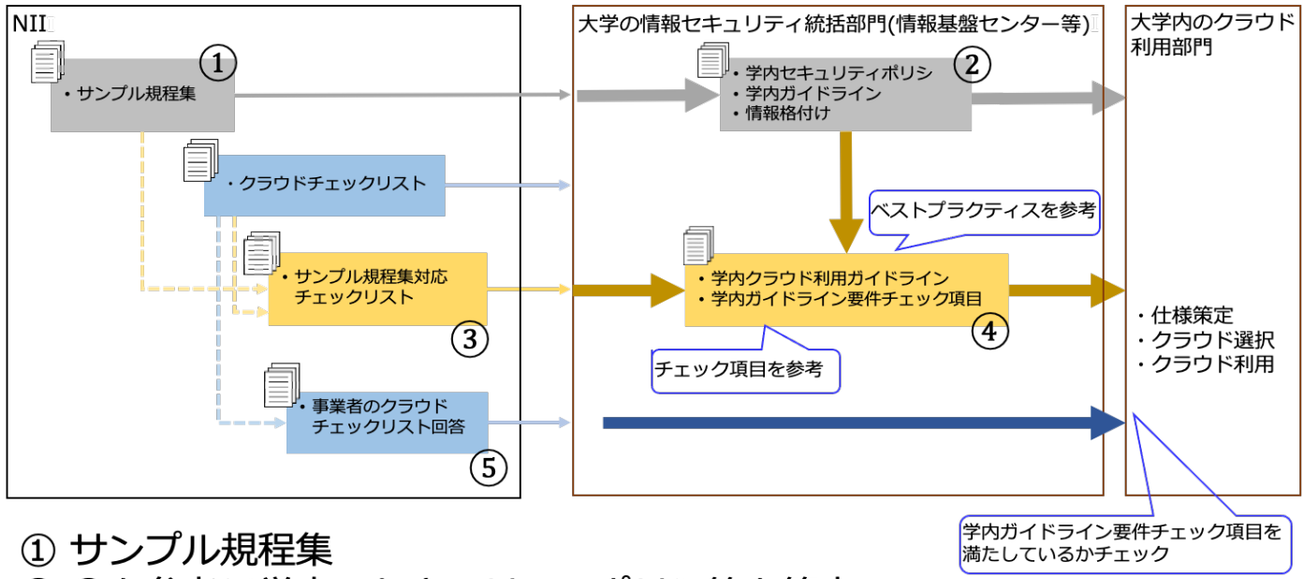
【注意事項】

1. 抽出したクラウドチェックリストの項目は、情報セキュリティ対策上、一般的にチェックしておく意味があると考えられる
「推奨参照項目」です。サンプル規程集に基づいて制定された実際の組織のセキュリティポリシ、パブリッククラウド上で
取り扱う情報の実際の格付け、パブリッククラウド上で運用するアプリケーションなどに応じて、参照する必要がない
チェックリスト項目あるいは他にも参照すべきチェックリスト項目があることに留意してください。

2. 「サンプル規程集の規定を満たすための施策案」(ベストプラクティス) は、読者が複雑な条件を考慮する負担を低減することを目的として、本資料作成時点の商用パブリッククラウドにおける情報セキュリティ関連の実装技術、運用、サービスレベル、サポートレベルを考慮して、どちらかと言えば安全側に倒した提案をしています。従って、実施の検討にあたっては、以下に留意してください。

- 実際の組織のセキュリティポリシ、取り扱う情報の実際の格付け、アプリケーションの種類や実装方法などによって、本施策案がどこまで適用できるかどうかという判断は変わる可能性があります。
- 実際のクラウドの利用にあたっては、費用と本施策案の実施をトレードオフしなければならない場合もあります。
- 適切な運用や使い方の対策を講じることによって、本施策案どおりでなくとも、組織のセキュリティポリシを満たすクラウド利用が可能となる場合もあります。
- 本施策案は、クラウド事業者のチェックリスト回答から調査した実際の商用クラウドにおける各項目の実現状況をふまえており、これらのクラウドを正しく設定して利用すれば比較的実現しやすいという点を考慮した提案を行っています。

【利用イメージ】



① サンプル規程集
② ①を参考に学内のセキュリティポリシ等を策定
③ サンプル規程集対応チェックリスト
④ ③を参考にして、②に基づいて学内のクラウド利用ガイドライン等を策定
⑤ 事業者のチェックリスト回答
(学認クラウド導入支援サービス参加機関の場合、参照可能)

【参考】

学認クラウド導入支援サービスでは、組織の情報基盤としてクラウドの導入を検討または計画している大学・研究機関の研究者や教職員を対象として、クラウドの導入・活用に関わる情報をまとめたスタートアップガイドを公開しています。
https://cloud.gakunin.jp/foracademy/#academy-02

D2101-	チェック項目	項番		詳細チェック項目	記入要領	サンプル規程集の規定を満たすための施策案	施策案を満たすチェックリスト回答	機密性	完全性	可用性
67	契約申込み	C	1	契約書の有無・その他の交付書面の種類	契約内容を明記する書面はあるか「Yes/No」欄を選択してください。Yesの場合は、その種類（契約書・約款等）と言語を記述回答欄に記入してください。（例：契約書（日本語）、サービス利用規約（英語）、など）	契約書あるいは約款などの形で契約内容・条件が明記された文書がカスタマに提供されるクラウドを利用する。	Yes	○	○	○
202 203	認証関連	D	2	SAML認証連携 (Shibboleth利用可否)	SAMLによるユーザ認証連携は可能か「Yes/No」欄を選択してください。 「Yes」の場合、Shibbolethによるユーザ認証連携の実績があれば記述回答欄に記入してください。 「No」の場合、SAML以外でユーザ認証連携可能なものがあれば記述回答欄に記入してください。	[要件に応じて検討] リモートアクセス端末あるいは利用者の認証において、学認利用のポリシがある場合には、SAML認証連携が可能なクラウドを利用する。	Yes/No	○		
98 202 203	認証関連	D	3	多要素認証	多要素認証に対応しているか「Yes/No」欄を選択してください。 「Yes」の場合、本人確認のためにどのような要素を用いているかを記述回答欄に記入してください。	リモートアクセス端末あるいは利用者の認証においては、多要素認証がサポートされているクラウドを利用する。 [利用側の施策] 極力、多要素認証を行う。 ※大学等で運用している多要素認証をサポートしている統合認証ソリューションを利用する場合は、それ経由で利用する個々のクラウドが統合認証サービスと適切に連携できるかどうかを確認するそのクラウド自体が多要素認証をサポートしているかどうかとは別に)。	Yes	○		
61 67 71	信頼性	E	1	サービス稼働率の規定	サービス稼働率を数値(例. 99.9%)で規定しているか「Yes/No」欄を選択してください。 「Yes」の場合、その値を記述回答欄に記入してください。また、SLAに規定している場合には、その旨を記入してください。	サービス稼働率が、SLAあるいはSLOとして、カスタマが参照可能な文書で明記されているクラウドを利用する。	Yes			○
71	信頼性	E	4	計画停止の有無	ユーザに影響を与える計画停止があるか「Yes/No」欄を選択してください。 「Yes」の場合、頻度および標準的な停止時間（例：〇時から〇時まで完全停止、〇時から〇時の間で5分程度停止など）を記述回答欄に記入してください。ここで、計画停止とは月次等の定期的なメンテナンスや法定停電による停止などのことです。	計画停止がないか(無停止保守を実現)、計画停止がある場合はその頻度・時間が明示され、事前にカスタマに通知されるクラウドを利用する。	Yes			○
76	サポート関連	F	1	サポート窓口	サポートについて、記述回答欄に以下を記入してください。サポートプラン（有償・無償など）毎に異なる場合はそれぞれについて記入してください。 ・窓口（例：メール、電話、チャット、など） ・受付時間帯（例：平日 9:00-17:00、24時間365日、など） ・回答時間（例：無償の標準プランの場合は1営業日以内、有償の〇〇プランの場合は4時間以内、など） ・対応言語（例：日本語のみ、日本語と英語、など）	サポートレベルに関する具体的な条件が契約書や約款等のカスタマが参照可能な文書で定められているクラウドを利用する。	記述回答に具体的な記述があるか、適切な情報源が示されている。			○
71	サポート関連	F	2	重要情報の通知	サービス停止、障害、保守実施、非互換を伴う仕様変更などの通知手順が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法（ウェブページに掲載（可能ならばURLを記入）、電子メール、契約時に書面で交付など）を記述回答欄に記入してください。	サービス停止、障害、保守実施、非互換を伴う仕様変更などの通知手順が、カスタマが参照可能な文書で定められている手順に従って事前に行われるクラウドを利用する。	Yes			○
49 141 191 202	ネットワーク・通信機能	G	1	SINET接続状況	SINETクラウド接続サービスを提供しているか「Yes/No」欄を選択してください。	[要件に応じて検討] 必要に応じて、SINETクラウド接続サービスを提供しているクラウドを利用し、L2VPNで接続する。	Yes/No	○	○	○
48 49 71 191 193 202 203	ネットワーク・通信機能	G	2	通信のセキュリティ確保	端末からサーバまでの通信のセキュリティ確保がサービスとして提供されているか「Yes/No」欄を選択してください。 「Yes」の場合、どのようにセキュリティを確保しているか、方式（SSHやSSL/TLSによる暗号化、ファイル共有におけるAES、SINET L2VPN、IPsec、SSL-VPN等）を記述回答欄に記入してください。	端末からサーバまでの通信に関して、「電子政府推奨暗号リスト」に記載された複数の暗号化アルゴリズムおよびそれに基づいた安全なプロトコルを選択することが可能なクラウドを利用する。 [追加策] VPN回線でクラウドを利用する場合、二重の暗号化を行う（例えば、インターネット VPN 回線において IPsec で通信経路の暗号化を行った上で HTTPS 通信によりコンテンツの暗号化を行 う)などを考慮する。	Yes	○		
114 140 163 189 197	ネットワーク・通信機能	G	4	アクセス制限機能	サーバを防衛するためのアクセス制限機能がサービスとして提供されているか「Yes/No」欄を選択してください。 「Yes」の場合、アクセス制限の単位（IPアドレス、ポート番号など）を記述回答欄に記入してください。	ネットワークのアクセス制限機能(ファイアウォール、セキュリティグループ、WAF [Web Application Firewall] 等) が提供されているクラウドを利用する。 [利用側の施策] これらの機能の設定を適切に行うことにより通信を制御する。	Yes	○		

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

114 141 192	ネットワーク・通信機能	G	6	専用ネットワークセグメント利用の可否	クラウド上にユーザ専用のネットワークセグメントを利用することができるか 「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください（事業者からの割り当て、ユーザによる作成など）。	ユーザ専用のネットワークセグメントを利用することが可能なクラウドを利用する。 [利用側の施策] ネットワークセグメントの分割を適切に設計・設定することによりアクセス制御を行う。	Yes	○		
114 141 191 194 203	ネットワーク・通信機能	G	8	IPアドレス制限の可否	ユーザはアクセス元のIPアドレスをもとにアクセス制御を行うことはできるか 「Yes/No」欄を選択してください。	アクセス元のIPアドレスに基づいてアクセス制御を行うことの可能なクラウドを利用する。 [利用側の施策] ネットワークセグメントの分割を適切に設計・設定することによりアクセス制御を行う。	Yes	○		
186	管理機能	H	1	管理者権限	ユーザは利用するサーバの管理者権限（Linux等：root権限、Windows：Administrator権限）を与えられるか「Yes/No」欄を選択してください。	管理者権限の与えられているクラウドを利用する。 [利用側の施策] 管理者アカウントの権限管理を適正に行う。	Yes	○		
93 208	管理機能	H	2	稼働状況の一覧表示機能	ユーザに割り当てられたプロセスの死活やリソースの使用率などのサービス稼働状況を一覧で表示する機能は提供されるか「Yes/No」欄を選択してください。	サービス稼働状況やネットワーク状況を確認できる機能が提供されているクラウドを利用する。 [利用側の施策] その機能を使用して運用状況を確認・記録し、それに基づいてサーバやネットワークの資源を適切に分配・管理する。	Yes			○
192	管理機能	H	4	ネットワーク構成機能	ユーザがネットワークの構成を変更する機能は提供されるか「Yes/No」欄を選択してください。	ネットワーク構成機能が提供されているクラウドを利用する。 [利用側の施策] 当機能によってVLANを構成することで通信経路を分離し、それぞれの通信を制御する。	Yes	○		○
159	管理機能	H	5	ロードバランサ利用可否	サーバ間でのロードバランサ機能は提供されるか「Yes/No」欄を選択してください。	[要件に応じて検討] 必要に応じて、ロードバランサ機能が提供されているクラウドの利用を検討する。	Yes/No			○
157 159	管理機能	H	6	フェイルオーバー機能の提供	サーバ間でのフェイルオーバー機能は提供されるか「Yes/No」欄を選択してください。 「Yes」の場合、災害対応など冗長性を考慮しているか記述回答欄に記入してください。	[要件に応じて検討] フェイルオーバー機能が提供されているクラウドの利用を検討する。 ※サーバが停止した場合に自動的に（正常なハードウェア上で）再起動される仕様となっているクラウドもあるので、RTOが厳しくない場合は、その機能を利用することも検討する。	Yes/No			○
93 208	管理機能	H	9	プロセス監視機能	ユーザに割り当てられたプロセスの死活やリソースの使用率の監視・アラート機能は提供されるか「Yes/No」欄を選択してください。	プロセスの監視・アラート機能が提供されているクラウドを利用する。 [利用側の施策] 当機能によって状況を確認し、サーバやネットワークの資源を適切に分配・管理する。	Yes			○
186	管理機能	H	10	IDとアクセス管理	ユーザ、およびユーザ権限の管理機能は提供されるか「Yes/No」欄を選択してください。	IDとアクセス管理機能（IDおよびそのIDの権限の管理機能）が提供されているクラウドを利用する。 [利用側の施策] 当機能によって、クラウドに格納された要機密情報のアクセス管理(ダウンロード等の操作も想定して)や、管理者アカウントの適正な権限管理を行う。	Yes	○		
196 208	管理機能	H	11	利用統計	サービスへのアクセス数やリソースの利用率など、利用統計を取得する機能は提供されるか「Yes/No」欄を選択してください。 「Yes」の場合、どのような統計が取得可能か記述回答欄に記入してください。	利用統計を取得できるクラウドを利用する。 [利用側の施策] 当機能によって通信回線の通信量、接続率等の運用状態を定常的に確認・記録・分析し、サーバやネットワークの資源を適切に分配・管理する。	Yes			○
208	スケーラビリティ	J	1	スペックレベル選択	ユーザがニーズに応じたサーバ構成を容易に選択できるように、CPUやメモリ、ストレージ等の初期構成を複数のメニューから選択することができるか 「Yes/No」欄を選択してください。	スペックレベルの選択が可能なクラウドを利用する。 [利用側の施策] 当機能によって利用者等の利用形態に応じて適切な構成を選択する。	Yes			○
43 54 55 57 157 158	データセンター	K	1	防犯設備	データセンターにはどのような防犯設備（監視カメラ、警備員常駐、侵入検知センサー、など）を備えているか記述回答欄に記入してください。	防犯設備の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。	記述回答に具体的な記述があるか、適切な情報源が示されている。	○	○	
54 157 158	データセンター	K	2	入退室管理体制	データセンターへの入退室をどのように管理（ICカード認証、生体認証、警備員による本人確認、など）しているか記述回答欄に記入してください。健康チェック（検温など）を行っている場合には記入してください。	入退室管理体制の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。	記述回答に具体的な記述があるか、適切な情報源が示されている。	○	○	

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

58	データセンター	K	3	防災対策	データセンターにはどのような防災対策（煙センサー、ガス消火装置、排水設備、など）が行われているか記述回答欄に記入してください。	防災対策の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。	記述回答に具体的な記述があるか、適切な情報源が示されている。			○
157 159	データセンター	K	4	電力障害対策	データセンターに電力が安定して供給されるよう、監視、二系統受電、自家発電などの対策を行っている場合は記述回答欄に記入してください。災害対応など冗長性を考慮しているか記入してください。	電力障害対策の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。	記述回答に具体的な記述があるか、適切な情報源が示されている。			○
157 159 191 196	データセンター	K	5	ネットワーク障害対策	データセンターのネットワークが安定して運用されるよう、監視や二重化などの対策を行っているか記述回答欄に記入してください。災害対応など冗長性を考慮しているか記入してください。	ネットワーク障害対策の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。 ※本項目は、クラウド基盤の冗長化に関するものであり、高可用性実現のためのシステムとしての冗長化は別途検討が必要である。	記述回答に具体的な記述があるか、適切な情報源が示されている。			○
53 60 61 70	データセンター	K	6	データセンターの設置地域	データセンターが設置されている地域やゾーン（同一地域内で冗長化されている独立したデータセンターに相当する単位）を公表していいるか「Yes/No」欄を選択してください。 「Yes」の場合、地域名やゾーン数を記述回答欄に記入してください。契約後のみ開示される場合はその旨を記入してください。また、国内にデータセンターが設置されている場合(あるいは設置されていることを公表可能な場合)は、その旨を記入してください。	データセンターの設置地域が公開されているクラウドを利用する。 [追加策] 要求されるデータの機密性によっては、データセンターが適切な地域（たとえば国内）に設置されているクラウドを利用する。	Yes	○	○	○
70	データセンター	K	7	地域・ゾーンの指定	どの地域・ゾーン（同一地域内で冗長化されている独立したデータセンターに相当する単位）にあるデータセンターを利用するか（ファイルの保存も含む）をユーザが指定することは可能か「Yes/No」欄を選択してください。	[要件に応じて検討] 要求されるデータの機密性に応じて、適切な地域・ゾーン（たとえば国内）に設置されているデータセンターを指定する。	Yes	○	○	○
60 61 71 87	セキュリティ（全般）	L	1	セキュリティポリシ	サービスの運用に関わるセキュリティポリシをユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法（ウェブページに掲載、契約時に書面で交付など）を記述回答欄に記入してください。	サービスの運用に関わるセキュリティポリシが、カスタマに文書として開示されているクラウドを利用する。	Yes	○	○	○
70	セキュリティ（全般）	L	2	ユーザが利用するリソースの分離	ユーザが利用するリソースは、他のユーザのリソースとどのレベルで分離されているか記述回答欄に記入してください（例：アプリケーション、VM、物理マシン）。	可能な限りリソースの分離方式が開示されているクラウドを利用する。 [利用側の施策] 以下のような分離レベルから生じるセキュリティリスクを理解して利用する。一般に、同一ハードウェア上でソフトウェアによって分離されているものは、当該ソフトウェアの脆弱性や他の利用者（テナント）からの攻撃によるリスクがないとは言えない。ハードウェアレベルで分離されていればこのようなリスクは軽減されるが、データセンターの内部ネットワークに対する攻撃などの可能性は残る。	記述回答に具体的な記述があるか、適切な情報源が示されている。	○	○	○
61 63 64 87 93	セキュリティ（全般）	L	3	インシデント対応（クラウド事業者管理のリソース）	クラウド事業者がサービスを提供するために用いるリソースにセキュリティインシデント（不正侵入、DoS攻撃、情報漏えいなど）が発生した場合の、事業者としての対応方針・方法をユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、ユーザが対応方針・方法を確認する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	インシデント発生時の対応方針や方法が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes	○	○	○
61 63 64 87	セキュリティ（全般）	L	4	インシデント対応（ユーザ管理のリソース）	ユーザが管理しているリソースにセキュリティインシデント（不正侵入、DoS攻撃、情報漏えいなど）が発生した場合の、事業者としての対応方針・方法をユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、対応方針・方法（何もしない、ユーザに対応を依頼、サービス強制停止など）を記述回答欄に記入してください。また、対応がオプションサービスとなる場合はその旨を記入してください。	インシデント発生時の対応方針や方法が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes	○	○	○
71 81 87 93 129 130	セキュリティ（全般）	L	5	バージョンアップの頻度	クラウド事業者がサービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、その頻度あるいは基準を記述回答欄に記入してください。	サービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes	○		○

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

81 93 129 130	セキュリティ（全般）	L	6	アップデート情報（脆弱性情報）の提供	サーバのメニュー、テンプレート、イメージとして提供されているOS・アプリケーション等のアップデート情報や脆弱性情報はユーザに提供されるか「Yes/No」欄を選択してください。	サービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準がカスタマに文書として開示されているクラウドを利用する。 [追加策] 利用しているサーバに対して可能な範囲で脆弱性診断を実施することを検討する。	Yes	○		○
129 130	セキュリティ（全般）	L	7	セキュリティアップデートの自動適用	サーバのメニュー、テンプレート、イメージとして提供されているOS・アプリケーション等の自動セキュリティアップデート機能はユーザに提供されるか 「Yes/No」欄を選択してください。	サーバのメニュー、テンプレート、イメージとして提供されているOS・アプリケーション等の自動セキュリティアップデート機能が利用者に提供されているクラウドを利用する。 [追加策] 利用しているサーバに対して可能な範囲で脆弱性診断を実施することを検討する。	Yes	○		○
67 71 131 134	セキュリティ（全般）	L	8	セキュリティ対策	ウイルス検知・防御のサービスが提供されているか「Yes/No」欄を選択してください（IaaS等でユーザが独自にソフトウェアを導入する場合を除く）。「Yes」の場合、基本サービスかオプションサービスかを記述回答欄に記入してください。	不正プログラム対策ソフトウェア(マルウェア検知・防御のサービスなど)が提供されているクラウドを利用し、当該サービスを使用する。 不正プログラム対策ソフトウェアが提供されていないクラウドの場合には、カスタマ側で不正プログラム対策ソフトウェアを導入するなどの対策を行った上で利用する。	Yes/No	○		
132 134	セキュリティ（全般）	L	9	ウイルス定義の更新	ウイルス検知・防御のサービスが提供されている場合、ウイルス定義ファイルの更新頻度をユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、ユーザが更新頻度を確認する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	不正プログラム対策ソフトウェア(マルウェア検知・防御のサービスなど)のウイルス定義ファイルの更新頻度を確認し、クラウドの不正プログラム対策ソフトウェア(ウイルス検知・防御のサービスなど)等及びその定義ファイルは、常に最新のものが利用可能となるように対策する。	Yes	○		
93 161 163 186 197	セキュリティ（全般）	L	10	ログ分析・脅威検出	ログ分析やセキュリティ上の脅威の自動検出を行う機能（SIEM(Security Information and Event Management)、CASB(Cloud Access Security Broker)等）が提供されるか「Yes/No」欄を選択してください。 「Yes」の場合、具体的な機能を記述回答欄に記入してください。	[要件に応じて検討] 内部および外部からの不正アクセスのチェック・分析の頻度や分析の精度を高める必要がある場合、専任の分析担当者の設置、ログ分析やセキュリティ上の脅威の自動検出を行う機能の利用、監視事業者への委託(F4, F5)を検討する 。	Yes/No	○	○	
93 161 163 186 197	セキュリティ（全般）	L	11	IDS・IPS	IDS（不正侵入検知システム）・IPS（不正侵入予防システム）はサービスとして提供されているか「Yes/No」欄を選択してください。	[要件に応じて検討] 必要に応じて、IDS（不正侵入検知システム）/IPS（不正侵入予防システム）が提供されているクラウドを利用し、当該機能を使用する。 IPS/IDSが提供されていないクラウドの場合には、カスタマ側でこれらのシステムを導入するなどの対策を行った上で利用する。	Yes/No	○	○	
71 117 163 186 203	データ管理	M	1	ログの知的財産権	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の知的財産権がクラウド事業者とユーザ（または契約大学）のいずれに帰属するか、契約書や約款等に明記されているか「Yes/No」欄を選択してください。 「Yes」の場合、契約大学・研究機関が文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	必要なログを取得するために、ログの知的財産権が利用者に帰属するクラウドを利用する。	Yes	○	○	○
66 71 92 93 117 161 163 186 203	データ管理	M	2	ログの使用権（閲覧等）	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の使用権（閲覧等）がユーザ（または契約大学・研究機関）に認められているか「Yes/No」欄を選択してください。 「Yes」の場合、閲覧できるログの種類を記述回答欄に記入してください。さらに閲覧するログをユーザがダウンロードして保管することが可能であれば記入してください。	必要なログを取得するために、利用するクラウドのログの使用権（閲覧等）が認められているクラウドを利用する。 [追加策/要件に応じて検討] 利用するクラウドの時刻設定が可能な場合には、タイムサーバなどを利用して基準となる時刻に同期させる。また、ログに時刻情報も記録されるように設定する。 データにアクセスした利用者を特定できるようなアクセスログを取得できるように設定する。 データベースの操作ログを取得できるように設定する。 VPN回線を利用してクラウドを利用する場合、主体認証ログを取得できるように設定し管理する。	Yes	○	○	○

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

71 93 117 161 163 186 203	データ管理	M	3	ログの使用（閲覧等）可能期間	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の使用（閲覧等）の可能期間が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、可能期間を記述回答欄に記入してください。また、大学・研究機関からの要請により、可能期間を延長または短縮することが可能な場合には、記入してください。	[利用側の施策] 利用するクラウドのログの使用（閲覧等）の可能期間を確認し、大学等で定めたログの保存期間中はログを管理できるようにする。サービスにおけるログの使用可能期間が大学等で定めた保存期間より短い場合には、ログをログサーバ等に保管し、定めたログの保存期間中はログを閲覧できるようにする。	Yes/No	○	○	○
43 71 125 126 186 190	データ管理	M	4	データの暗号化	保存するユーザのデータは暗号化が可能か「Yes/No」欄を選択してください。 「Yes」の場合、暗号化する方式を記述回答欄に記入してください（ユーザが暗号化の要否を選択する、システムが自動で暗号化するなど）。	トランザクションデータおよび保存データの両方に関して「電子政府推奨暗号リスト」に記載された複数の暗号化アルゴリズムおよびそれに基づいた安全なプロトコルを選択することが可能なクラウドを利用する。	Yes	○		
125 126 186 190	データ管理	M	5	暗号化鍵の管理方法	ユーザのデータ管理において暗号化に用いる鍵の管理方法は公開されているか「Yes/No」欄を選択してください。 「Yes」の場合、ユーザが確認する方法を記述回答欄に記入してください。	トランザクションデータおよび保存データの両方に関して暗号化が可能なクラウドを利用する場合、暗号化に用いる鍵の管理方法について確認する。 [追加策] カスタマによる鍵管理が可能な場合は、必要に応じて、鍵管理を自前で行うことを検討する。	Yes	○		
39 67 157	データ管理	M	6	データの多重化	ユーザが格納したデータは多重化されているか「Yes/No」欄を選択してください。 「Yes」の場合、どのような手法か（RAID、複数データセンターに保存など）記述回答欄に記入してください。災害対応など冗長性を考慮しているか記入してください。	格納データがデータセンタ内で多重化されているサービスを利用する。 [追加策] 必要に応じて、データセンタ間で多重化されている（あるいは多重化可能な）クラウドを利用する。	Yes			○
42 43 114 119	データ管理	M	7	データのアクセス制限	ユーザが格納したデータごと（例えばファイルごと）にアクセス制限のレベルを任意に設定することができるか「Yes/No」欄を選択してください。 「Yes」の場合、アクセス制限はどのように行っているか記述回答欄に記入してください（GUIで操作、スクリプトで記述など）。	ファイルやオブジェクトなどのデータの取扱い単位ごとにID・アクセス管理機能を持つクラウドを利用する。 [利用側の施策] データに対するアクセス権限を極力細分化した上で、当機能によって、必要最小限の利用者だけにアクセス権限を与えるよう管理・制御する。	Yes	○		
39 43 156	データ管理	M	9	データのローカルコピー保持と同期	クラウド上に格納されたデータに対してクライアント側にローカルコピーをもつことは可能か「Yes/No」欄を選択してください。 「Yes」の場合、クラウド上のデータとの同期のタイミングや同期処理の性能について記述回答欄に記入してください。	クライアント側にローカルコピーを作成しない、あるいは作成することを抑止できるクラウドを利用する。 [利用側の施策] 後者の場合は、抑止機能を使用する。	Yes/No	○		
39 43 51 66 161 164	バックアップ	N	1	バックアップサービスの有無	ユーザがクラウドに格納したデータあるいはユーザが作成したサーバイメージのバックアップを行うサービスは提供されているか「Yes/No」欄を選択してください。（管理者権限をもったユーザのスクリプト等による実現は除く）。	バックアップサービスを提供しているクラウドの場合はその機能を利用する。 提供していないクラウドの場合は、利用者側でバックアップを取得する。	Yes/No	○		○
51 164	バックアップ	N	3	バックアップの世代管理	複数世代のバックアップを取得・管理することは可能か「Yes/No」欄を選択してください。 「Yes」の場合、世代数の上限やフルバックアップ・差分バックアップの選択は可能か記述回答欄に記入してください。	[要件に応じて検討] クラウドが提供するバックアップサービスを利用する際に、複数世代のバックアップ取得・管理が必要な場合には本機能を利用する。	Yes/No			○
53 164	バックアップ	N	4	複数センターへの同時バックアップ可否	バックアップ先として同一インフラストラクチャ、別インフラストラクチャ、別データセンタ、別地域などを指定することは可能か「Yes/No」欄を選択してください。 「Yes」の場合、これらの複数のバックアップ先のバックアップデータの一貫性を維持することは可能か記述回答欄に記入してください。また、特に災害対応を考慮する場合、バックアップ先をどのように指定すればよいか記入してください。	[要件に応じて検討] クラウドが提供するバックアップサービスを利用する際に、複数のセンターへの同時バックアップが必要な場合は本機能を利用する。	Yes/No			○
161 164	バックアップ	N	5	バックアップからのリストア	バックアップデータのリストアはユーザ自身で作業できるか「Yes/No」欄を選択してください。 「No」の場合、クラウド事業者作業の依頼手順を記述回答欄に記入してください。	バックアップデータのリストアをカスタマ自身で作業できるクラウドであれば、カスタマ自身の作業を前提としたリカバリ計画を策定する。 バックアップデータのリストアをカスタマ側で作業できないクラウドの場合、リストア作業を行う主体やその仕様（作業手順、タイミング等）について確認した上で利用する。	Yes/No			○

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

39 51 70 190	バックアップ	N	6	バックアップデータのセキュリティ	バックアップデータのアクセス制限や暗号化に関して、元のデータと同等のセキュリティレベルが継承されているか「Yes/No」欄を選択してください。	バックアップデータに対して元データと同等のセキュリティレベルが実現されるクラウドを利用する。 [利用側の施策] 必要な場合はそれが可能となる設定や利用方法を実施する。	Yes	○		
61	クラウド事業者の信頼性	O	1	経営状況	株式上場は行っているか「Yes/No」欄を選択してください。 「Yes」の場合、市場名も記述回答欄に記入してください。親会社が上場している場合はそちらについても記入してください。	サービスを提供する企業あるいはその親会社が株式上場等によって経営状況を開示しているクラウド、あるいは公的機関が提供するクラウドを極力利用する。	Yes	○		○
61 71	クラウド事業者の信頼性	O	2	プライバシポリシ	サービスの提供・運用に関わるプライバシポリシをユーザに提示しているか「Yes/No」欄を選択してください。	サービスの提供・運用に関わるプライバシポリシが、契約書や約款等のカスタマが参照可能な文書で定められているクラウドを利用する。	Yes	○		
61	クラウド事業者の信頼性	O	3	第三者委託	サービスの実施について第三者への委託を行っているか「Yes/No」欄を選択してください。 「Yes」の場合、委託先での法令や各種ポリシ順守について文書で定められているか記述回答欄に記入してください。定められている場合、契約大学・研究機関がその文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記入してください。	第三者委託を行っている場合、委託先での法令や各種ポリシ順守について文書で定められており、カスタマにその事実が開示されているクラウドを利用する。	Yes/No	○		
61 63 71	クラウド事業者の信頼性	O	4	ユーザによる監査	ユーザ自身の認証取得のため、ユーザがサービスを監査することは可能か「Yes/No」欄を選択してください。 「Yes」の場合、何の監査が可能か記述回答欄に記入してください。	カスタマによる監査を受け入れるか、それが不可能でも第三者による監査結果がカスタマに開示可能であるクラウドを利用する。	Yes/No	○	○	○
70	クラウド事業者の信頼性	O	5	サービスの監査結果の開示	提供しているサービスが認証取得などのために外部監査を受けている場合、監査結果を開示しているか「Yes/No」欄を選択してください。 「Yes」の場合、受けた外部監査の種類を記述回答欄に記入してください。	第三者による監査結果をカスタマに開示しているか、あるいは請求によって開示可能であるクラウドを利用する。	Yes	○	○	○
70	クラウド事業者の信頼性	O	6	国内法人 / 国内総代理店等の有無	（海外に主たる拠点を置く事業者のみ回答）日本国内法人もしくは国内総代理店など、国内に営業やサポートの窓口となる組織を有しているか「Yes/No」欄を選択してください。	国内に営業やサポートの窓口となる組織を有しているクラウドを利用する。	Yes			○
70 92	契約条件	P	1	責任範囲の明確化	クラウド事業者と大学（ないしエンドユーザ）の責任分界点は文書で定められているか「Yes/No」欄を選択してください。	責任分界点が、契約書や約款等のカスタマが参照可能な文書で定められているクラウドを利用する。	Yes	○	○	○
67 71	契約条件	P	2	契約条件・SLAの変更手続き	契約期間中に、クラウド事業者が契約条件やSLAの変更を行う場合の手続きが文書で定められているか「Yes/No」欄を選択してください。 「Yes」の場合、契約大学・研究機関がその文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	契約条件やSLAの変更手続きが、契約書や約款等のカスタマが参照可能な文書で定められているクラウドを利用する。	Yes	○	○	○
70	契約条件	P	4	準拠法	係争時の準拠法は日本法か「Yes/No」欄を選択してください。 「No」の場合、国・州名を記述回答欄に記入してください。	係争時の準拠法が日本法であるクラウドを利用する。	Yes	○	○	○
70	契約条件	P	5	管轄裁判所	指定管轄裁判所はあるか「Yes/No」欄を選択してください。 「Yes」の場合、管轄裁判所を記述回答欄に記入してください。	指定管轄裁判所が日本国内の裁判所であるクラウドを利用する。	Yes	○	○	○
70 71	契約条件	P	6	事業終了の告知時期	クラウド事業者が事業を終了する場合、何か月前に終了を告知されるかが契約書や約款などの文書に定められているか「Yes/No」欄を選択してください。 「Yes」の場合、契約大学・研究機関がその文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	事業終了の告知が、カスタマ側が対応するのに十分な時間的余裕をもって行われる(たとえば6か月以前)であることが、契約書や約款等のカスタマが参照可能な文書で定められているクラウドを利用する。	Yes			○
61	データの取り扱い	Q	1	データの知的財産権／使用権	ユーザがクラウドに格納したデータの知的財産権や使用権がクラウド事業者側には生じないことが契約書や約款等に明記されているか「Yes/No」欄を選択してください。 「Yes」の場合、契約大学・研究機関が文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	カスタマがクラウドに格納したデータの知的財産権や使用権がクラウド事業者側には生じないことが契約書や約款等に明記されているクラウドを利用する。	Yes	○		
50 63 64 67 71 94 165 201	データの取り扱い	Q	2	データの削除	ユーザがデータを明に削除した時の当該データ、あるいはユーザの都合により契約を終了した後のユーザ情報およびユーザが所有していた全データが再利用されないことが保証されているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください（例：NIST-SP-800-88に準拠した方法でデータをすべて削除する、など）。削除証明書の発行が可能な場合には記入してください。	カスタマによるデータ削除時の当該データやカスタマの契約終了後のカスタマ情報およびカスタマ所有データが、復元不可能な方法で削除されることが保証されるクラウドを利用する（データの削除証明書を発行してくれるクラウド事業者もある）。 [利用側の施策] カスタマがデータの削除を行う場合は、クラウド事業者から提示された当該データを復元不可能とする削除方法に従って削除を実施する。	Yes	○	○	

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

70 71 94	リソースの引継ぎ	R	1	契約終了時のデータの移行支援	ユーザの都合により契約を終了した時、ユーザがデータ移行の支援を受けることは可能か「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください。	データ移行の支援が受けられるクラウドを利用するか、あるいはクラウドからのデータの取出し方法に関して一括ダウンロードコマンド等の機能およびドキュメンテーションが完備しているクラウドを利用する。	Yes/No			○
70 71	リソースの引継ぎ	R	2	サービス利用終了時のデータ確保	ユーザの都合により契約を終了する時やクラウド事業者が事業を終了する時、サービス利用終了前にユーザがデータを完全な形で取り出す方法が担保されているか「Yes/No」欄を選択してください。 「Yes」の場合、データの取得方法（ダウンロード、物理媒体の提供等）を記述回答欄に記入してください。	データ移行の支援が受けられるクラウド、あるいはクラウドからのデータの取出し方法に関して一括ダウンロードコマンド等の機能およびドキュメンテーションが完備しているクラウドを利用する。	Yes			○
70 71	リソースの引継ぎ	R	3	サーバイメージの移行性	サーバイメージをオンプレミスの環境や他社クラウドにダウンロードして動作させることは可能か「Yes/No」欄を選択してください。 「Yes」の場合、条件・方法について記述回答欄に記入してください。	サーバイメージに関してオンプレミスの仮想環境や他社クラウドと互換性のあるクラウドを利用する。 [別案] 移行が必要となる可能性のあるアプリケーションに関しては、コンテナを利用する。	Yes/No			○
70 71	リソースの引継ぎ	R	4	ユーザデータの移行性	オンプレミスの環境や他社クラウドにユーザデータを移行することが可能か「Yes/No」欄を選択してください。 「Yes」の場合、何らかの移行ツールや手段は提供されるか記述回答欄に記入してください。	データ移行の支援が受けられるクラウド、あるいはクラウドからのデータの取出し方法に関して一括ダウンロードコマンド等の機能およびドキュメンテーションが完備しているクラウドを利用する。	Yes			○
60 70 76	第三者認証	S	3	セキュリティ	当該のサービスに携わる部署は、セキュリティに関する第三者認証など（プライバシーマーク、ISO 27001、ISO 27017、ISO 27018など）を取得しているか「Yes/No」欄を選択してください。 「Yes」の場合、取得している第三者認証を記述回答欄に記入してください。（書き方ガイド「記入対象となる第三者認証」参照。）	プライバシーマーク、ISO 27001、ISO 27017、ISO 27018、あるいはそれらに準ずる第三者認証を取得しているクラウドを利用する。	Yes	○	○	○
70 76	第三者認証	S	4	経営・事業	経営・事業に関する第三者認証（SOC1、ISO 14001など）を取得しているか「Yes/No」欄を選択してください。 「Yes」の場合、取得している第三者認証を記述回答欄に記入してください。（書き方ガイド「記入対象となる第三者認証」参照。）	SOC1、ISO 14001、あるいはそれらに準ずる第三者認証を取得しているクラウドを利用する。	Yes	○	○	○
94 165 201	セキュリティポリシ固有	SA	1	保守を目的としたストレージ機器などの物理的廃棄	サーバやストレージ機器の廃棄や故障による交換を行う場合、内蔵HDD/SSDなどのデータの保存媒体をデータの復元が不可能な方法(物理的破壊、消磁、暗号化キーの廃棄など)で処分しているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください（例：NIST-SP-800-88に準拠した方法でデータをすべて削除する、など）。また、処分を第三者に委託する場合は、データの復元が不可能な方法で処理されたことを監査しているかどうか記入してください。削除証明書の発行が可能な場合には記入してください。	クラウド事業者によるサーバやストレージ機器の廃棄時にデータの復元が不可能な方法で処理されることが保証されるクラウドを利用する。	—	○		

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

章	節	D2101-	「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(2019 年度版)」対応条文	チェック項目	項番		詳細チェック項目	記入要領	サンプル規程集の規定を満たすための施策案	施策案を満たすチェックリスト回答
第六章 情報の取扱い	第一節 情報の取扱い	39	D2101-39 (格付と取扱制限の継承、見直しに係る規定の整備)(政府機関統一基準の対応項番3.1.1(1)-4)(p.35) 第三十九条 全学実施責任者は、情報の加工時、複製時等における格付及び取扱制限の継承、見直しについて、以下を例に、規定を整備すること。D2101 情報セキュリティ対策基準 四 情報を複製する場合には、元となる情報の機密性に係る格付及び取扱制限を継承する。 五 完全性及び可用性については、作成時又は複製時に適切な格付を決定する。	データ管理	M	6	データの多重化	ユーザが格納したデータは多重化されているか 「Yes/No」欄を選択してください。 「Yes」の場合、どのような手法か(RAID、複数データセンターに保存など)記述回答欄に記入してください。災害対応など冗長性を考慮しているか記入してください。	格納データがデータセンタ内で多重化されているサービスを利用する。 [追加策] 必要に応じて、データセンタ間で多重化されている(あるいは多重化可能な) クラウドを利用する。	Yes
				データ管理	M	9	データのローカルコピー保持と同期	クラウド上に格納されたデータに対してクライアント側にローカルコピーをもつことは可能か「Yes/No」欄を選択してください。 「Yes」の場合、クラウド上のデータとの同期のタイミングや同期処理の性能について記述回答欄に記入してください。	クライアント側にローカルコピーを作成しない、あるいは作成することを抑止できるクラウドを利用する。 [利用側の施策] 後者の場合は、抑止機能を使用する。	Yes/No
				バックアップ	N	1	バックアップサービスの有無	ユーザがクラウドに格納したデータあるいはユーザが作成したサーバイメージのバックアップを行うサービスは提供されているか「Yes/No」欄を選択してください。(管理者権限をもったユーザのスクリプト等による実現は除く)。	バックアップサービスを提供しているクラウドの場合はその機能を利用する。 提供していないクラウドの場合は、利用者側でバックアップを取得する。	Yes/No
				バックアップ	N	6	バックアップデータのセキュリティ	バックアップデータのアクセス制限や暗号化に関して、元のデータと同等のセキュリティレベルが継承されているか「Yes/No」欄を選択してください。	バックアップデータに対して元データと同等のセキュリティレベルが実現されるクラウドを利用する。 [利用側の施策] 必要な場合はそれが可能となる設定や利用方法を実施する。	Yes
		42	D2101-42 (情報の利用・保存)(政府機関統一基準の対応項番 3.1.1(4))(p.40) 第四十二条 教職員等は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うこと。 4 教職員等は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること。	データ管理	M	7	データのアクセス制限	ユーザが格納したデータごと(例えばファイルごと)にアクセス制限のレベルを任意に設定することができるか 「Yes/No」欄を選択してください。 「Yes」の場合、アクセス制限はどのように行っているか記述回答欄に記入してください(GUIで操作、スクリプトで記述など)。	ファイルやオブジェクトなどのデータの取扱い単位ごとにID・アクセス管理機能を持つクラウドを利用する。 [利用側の施策] データに対するアクセス権限を極力細分化した上で、当機能によって、必要最小限の利用者だけにアクセス権限を与えるよう管理・制御する。	Yes
		43	D2101-43 (格付と取扱制限に応じた情報の取り扱い)(政府機関統一基準の対応項番 3.1.1(4)-1 (p.42) 第四十三条 教職員等は、情報の格付及び取扱制限に応じて、情報を以下のとおり取り扱うこと。 二 要機密情報を必要以上に複製しない。 三 電磁的記録媒体に要機密情報を保存する場合には、主体認証情報を用いて保護するか又は情報を暗号化したり、施錠のできる書庫・保管庫に媒体を保存したりするなどの措置を講ずる。 五 情報の保存方法を変更する場合には、格付、取扱制限及び記録媒体の特性に応じて必要な措置を講ずる。	データセンター	K	1	防犯設備	データセンターにはどのような防犯設備(監視カメラ、警備員常駐、侵入検知センサー、など)を備えているか記述回答欄に記入してください。	防犯設備の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する(たとえばJDCC tier3 (相当))。	記述回答に具体的な記述があるか、適切な情報源が示されている。
				データ管理	M	4	データの暗号化	保存するユーザのデータは暗号化が可能か「Yes/No」欄を選択してください。 「Yes」の場合、暗号化する方式を記述回答欄に記入してください(ユーザが暗号化の要否を選択する、システムが自動で暗号化するなど)。	トランザクションデータおよび保存データの両方に関して「電子政府推奨暗号リスト」に記載された複数の暗号化アルゴリズムおよびそれに基づいた安全なプロトコルを選択することが可能なクラウドを利用する。	Yes
				データ管理	M	7	データのアクセス制限	ユーザが格納したデータごと(例えばファイルごと)にアクセス制限のレベルを任意に設定することができるか 「Yes/No」欄を選択してください。 「Yes」の場合、アクセス制限はどのように行っているか記述回答欄に記入してください(GUIで操作、スクリプトで記述など)。	ファイルやオブジェクトなどのデータの取扱い単位ごとにID・アクセス管理機能を持つクラウドを利用する。 [利用側の施策] データに対するアクセス権限を極力細分化した上で、当機能によって、必要最小限の利用者だけにアクセス権限を与えるよう管理・制御する。	Yes
				データ管理	M	9	データのローカルコピー保持と同期	クラウド上に格納されたデータに対してクライアント側にローカルコピーをもつことは可能か「Yes/No」欄を選択してください。 「Yes」の場合、クラウド上のデータとの同期のタイミングや同期処理の性能について記述回答欄に記入してください。	クライアント側にローカルコピーを作成しない、あるいは作成することを抑止できるクラウドを利用する。 [利用側の施策] 後者の場合は、抑止機能を使用する。	Yes/No
				バックアップ	N	1	バックアップサービスの有無	ユーザがクラウドに格納したデータあるいはユーザが作成したサーバイメージのバックアップを行うサービスは提供されているか「Yes/No」欄を選択してください。(管理者権限をもったユーザのスクリプト等による実現は除く)。	バックアップサービスを提供しているクラウドの場合はその機能を利用する。 提供していないクラウドの場合は、利用者側でバックアップを取得する。	Yes/No
		48	D2101-48 (情報漏えいの防止、情報の改ざんの防止)(政府機関統一基準の対応項番3.1.1(6)-1,2)(p.44) 第四十八条 教職員等は、要機密情報である電磁的記録を要管理対策区域外に運搬又は学外通信回線を使用して送信する場合には、情報漏えいを防止するため、以下を例とする対策を講ずること。 一 運搬又は送信する情報を暗号化する。	ネットワーク・通信機能	G	2	通信のセキュリティ確保	端末からサーバまでの通信のセキュリティ確保がサービスとして提供されているか「Yes/No」欄を選択してください。 「Yes」の場合、どのようにセキュリティを確保しているか、方式(SSHやSSL/TLSによる暗号化、ファイル共有におけるAES、SINET L2VPN、IPsec、SSL-VPN等)を記述回答欄に記入してください。	端末からサーバまでの通信に関して、「電子政府推奨暗号リスト」に記載された複数の暗号化アルゴリズムおよびそれに基づいた安全なプロトコルを選択することが可能なクラウドを利用する。 [追加策] VPN回線でクラウドを利用する場合、二重の暗号化を行う(例えば、インターネット VPN 回線において IPsec で通信経路の暗号化を行った上で HTTPS 通信によりコンテンツの暗号化を行 う)などを考慮する。	Yes
		49	D2101-49 (情報の送信に係る対策)(政府機関統一基準の対応項番 3.1.1(6)-4)(p.45) 第四十九条 教職員等は、要保護情報である電磁的記録を送信する場合は、安全確保に留意して、以下を例に当該情報の送信の手段を決定すること。	ネットワーク・通信機能	G	1	SINET接続状況	SINETクラウド接続サービスを提供しているか「Yes/No」欄を選択してください。	[要件に応じて検討] 必要に応じて、SINETクラウド接続サービスを提供しているクラウドを利用し、L2VPNで接続する。	Yes/No

国立情報学研究所 クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

			二 信頼できる通信回線を使用して送信する。 三 VPN を用いて送信する。	ネットワーク・通信機能	G	2	通信のセキュリティ確保	端末からサーバまでの通信のセキュリティ確保がサービスとして提供されているか「Yes/No」欄を選択してください。 「Yes」の場合、どのようにセキュリティを確保しているか、方式（SSHやSSL/TLSによる暗号化、ファイル共有におけるAES、SINET L2VPN、IPsec、SSL-VPN等）を記述回答欄に記入してください。	端末からサーバまでの通信に関して、「電子政府推奨暗号リスト」に記載された複数の暗号化アルゴリズムおよびそれに基づいた安全なプロトコルを選択することが可能なクラウドを利用する。 [追加策] VPN回線でクラウドを利用する場合、二重の暗号化を行う（例えば、インターネット VPN 回線において IPsec で通信経路の暗号化を行った上で HTTPS 通信によりコンテンツの暗号化を行 う)などを考慮する。	Yes
		50	D2101-50（情報の消去）（政府機関統一基準の対応項番 3.1.1(7)）(p.45) 第五十条 教職員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。 2 教職員等は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。 3 教職員等は、要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。	データの取り扱い	Q	2	データの削除	ユーザがデータを明に削除した時の当該データ、あるいはユーザの都合により契約を終了した後のユーザ情報およびユーザが所有していた全データが再利用されないことが保証されているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください（例：NIST-SP-800-88に準拠した方法でデータをすべて削除する、など）。削除証明書の発行が可能な場合には記入してください。	カスタマによるデータ削除時の当該データやカスタマの契約終了後のカスタマ情報およびカスタマ所有データが、復元不可能な方法で削除されることが保証されるクラウドを利用する（データの削除証明書を発行してくれるクラウド事業者もある）。 [利用側の施策] カスタマがデータの削除を行う場合は、クラウド事業者から提示された当該データを復元不可能とする削除方法に従って削除を実施する。	Yes
		51	D2101-51（情報のバックアップ）（政府機関統一基準の対応項番 3.1.1(8)）(p.47) 第五十一条 教職員等は、情報の格付に応じて、適切な方法で情報のバックアップを実施すること。 2 教職員等は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理すること。 3 教職員等は、保存期間を過ぎた情報のバックアップについては、前条の規定に従い、適切な方法で消去、抹消又は廃棄すること。	バックアップ	N	1	バックアップサービスの有無	ユーザがクラウドに格納したデータあるいはユーザが作成したサーバイメージのバックアップを行うサービスは提供されているか「Yes/No」欄を選択してください。（管理者権限をもったユーザのスクリプト等による実現は除く）。	バックアップサービスを提供しているクラウドの場合はその機能を利用する。 提供していないクラウドの場合は、利用者側でバックアップを取得する。	Yes/No
				バックアップ	N	3	バックアップの世代管理	複数世代のバックアップを取得・管理することは可能か「Yes/No」欄を選択してください。 「Yes」の場合、世代数の上限やフルバックアップ・差分バックアップの選択は可能か記述回答欄に記入してください。	[要件に応じて検討] クラウドが提供するバックアップサービスを利用する際に、複数世代のバックアップ取得・管理が必要な場合には本機能を利用する。	Yes/No
				バックアップ	N	6	バックアップデータのセキュリティ	バックアップデータのアクセス制限や暗号化に関して、元のデータと同等のセキュリティレベルが継承されているか「Yes/No」欄を選択してください。	バックアップデータに対して元データと同等のセキュリティレベルが実現されるクラウドを利用する。 [利用側の施策] 必要な場合はそれが可能となる設定や利用方法を実施する。	Yes
		53	D2101-53（ 要保全情報又は要安定情報のバックアップ）（ 政府機関統一基準の対応項番3.1.1(8)-2）(p.47) 第五十三条 教職員等は、要保全情報、要安定情報である電磁的記録のバックアップ又は重要な設計書のバックアップの保管について、災害等により生ずる業務上の支障を考慮し、適切な保管場所を選定すること。	データセンター	K	6	データセンターの設置地域	データセンターが設置されている地域やゾーン（同一地域内で冗長化されている独立したデータセンターに相当する単位）を公表していいるか「Yes/No」欄を選択してください。 「Yes」の場合、地域名やゾーン数を記述回答欄に記入してください。契約後のみ開示される場合はその旨を記入してください。また、国内にデータセンターが設置されている場合(あるいは設置されていることを公表可能な場合)は、その旨を記入してください。	データセンターの設置地域が公開されているクラウドを利用する。 [追加策] 要求されるデータの機密性によっては、データセンターが適切な地域（たとえば国内）に設置されているクラウドを利用する。	Yes
				バックアップ	N	4	複数センターへの同時バックアップ可否	バックアップ先として同一インフラストラクチャ、別インフラストラクチャ、別データセンタ、別地域などを指定することは可能か「Yes/No」欄を選択してください。 「Yes」の場合、これらの複数のバックアップ先のバックアップデータの一貫性を維持することは可能か記述回答欄に記入してください。また、特に災害対応を考慮する場合、バックアップ先をどのように指定すればよいか記入してください。	[要件に応じて検討] クラウドが提供するバックアップサービスを利用する際に、複数のセンターへの同時バックアップが必要な場合は本機能を利用する。	Yes/No
		54	D2101-54（要管理対策区域における対策の基準の決定）（政府機関統一基準の対応項番 3.2.1(1)）(p.48) 第五十四条 全学実施責任者は、要管理対策区域の範囲を定めること。 2 全学実施責任者は、要管理対策区域の特性に応じて、以下の観点を含む対策の基準を定めること。 一 許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策。 二 許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策。	データセンター	K	1	防犯設備	データセンターにはどのような防犯設備（監視カメラ、警備員常駐、侵入検知センサー、など）を備えているか記述回答欄に記入してください。	防犯設備の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。	記述回答に具体的な記述があるか、適切な情報源が示されている。
				データセンター	K	2	入退室管理体制	データセンターへの入退室をどのように管理（ICカード認証、生体認証、警備員による本人確認、など）しているか記述回答欄に記入してください。健康チェック（検温など）を行っている場合には記入してください。	入退室管理体制の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。	記述回答に具体的な記述があるか、適切な情報源が示されている。

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

		55	D2101-55（要管理対策区域における対策）（政府機関統一基準の対応項番 3.2.1(1)-1,2,3,4,5）(p.49) 第五十五条 全学実施責任者は、以下を例とする、要管理対策区域の安全性を確保するための段階的な対策の水準（以下「クラス」という。）を定めること。 一 下表のとおり、3段階のクラスを定める。 クラス 説明 クラス3 一部の限られた者以外の者の立入りを制限する必要があるなど、クラス2より強固な情報セキュリティを確保するための厳重な対策を実施する必要がある区域 クラス2 教職員等以外の者の立入りを制限する必要があるなど、情報セキュリティを確保するための対策を実施する必要がある区域 クラス1 クラス3、クラス2以外の要管理対策区域 4 全学実施責任者は、クラス3の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。 一 クラス3の区域への立入りを許可されていない者の立入り等を防止するために、壁、常時施錠された扉、固定式のパーティション等強固な境界で下位のクラスの区域と明確に区分すること。 二 クラス3の区域へ許可されていない者が立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置を講ずること。 三 クラス3の区域への立入りを許可されていない者に、不必要に情報を与えないために、区域の外側から内部の重要な情報や情報システムが見えないようにすること。 四 一時的に立ち入った者が不正な行為を行うことを防止するために、一時的に立ち入った者を放置しないなどの措置を講ずること。業者が作業を行う場合は立会いや監視カメラ等により監視するための措置を講ずること。 5 全学実施責任者は、以下を例とする、区域へのクラスの割当ての基準を定めること 一 クラスの割当ての基準を以下のように定める。 ・ サーバ室や日常的に機密性が高い情報を取り扱う 研究室、事務室には、一部の限られた者以外の者が立ち入り盗難又は破壊をすること、情報システムを直接操作して情報窃取すること等を防止するために、クラス3を割り当てる。	データセンター	K	1	防犯設備	データセンターにはどのような防犯設備（監視カメラ、警備員常駐、侵入検知センサー、など）を備えているか記述回答欄に記入してください。	防犯設備の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。	記述回答に具体的な記述があるか、適切な情報源が示されている。
		57	D2101-57（区域ごとの対策）（政府機関統一基準の対応項番 3.2.1(2)-1）(p.55) 第五十七条 区域情報セキュリティ責任者は、管理する区域において、クラスの割当ての基準を参考にして当該区域に割り当てるクラスを決定するとともに、決定したクラスに対して定められた対策の基準と、周辺環境や当該区域で行う教育研究事務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。この際、決定したクラスで求められる対策のみでは安全性が確保できない場合は、当該区域で実施する個別の対策を含め決定すること。	データセンター	K	1	防犯設備	データセンターにはどのような防犯設備（監視カメラ、警備員常駐、侵入検知センサー、など）を備えているか記述回答欄に記入してください。	防犯設備の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。	記述回答に具体的な記述があるか、適切な情報源が示されている。
		58	D2101-58（要管理対策区域における対策の実施）（政府機関統一基準の対応項番 3.2.1(3)）(p.56) 第五十八条 区域情報セキュリティ責任者は、管理する区域に対して定めた対策を実施すること。 2 区域情報セキュリティ責任者は、災害から要安定情報を取り扱う情報システムを保護するために物理的な対策を講ずること。	データセンター	K	3	防災対策	データセンターにはどのような防災対策（煙センサー、ガス消火装置、排水設備、など）が行われているか記述回答欄に記入してください。	防災対策の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。	記述回答に具体的な記述があるか、適切な情報源が示されている。
第七章 外部委託	第一節 外部委託	60	D2101-60（外部委託に係る規定の整備）（政府機関統一基準の対応項番 4.1.1(1)）(p.59) 第六十条 全学実施責任者は、外部委託に係る以下の内容を含む規定を整備すること。 一 委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準 二 委託先の選定基準	データセンター	K	6	データセンターの設置地域	データセンターが設置されている地域やゾーン（同一地域内で冗長化されている独立したデータセンターに相当する単位）を公表していいるか「Yes/No」欄を選択してください。 「Yes」の場合、地域名やゾーン数を記述回答欄に記入してください。契約後のみ開示される場合はその旨を記入してください。また、国内にデータセンターが設置されている場合（あるいは設置されていることを公表可能な場合）は、その旨を記入してください。	データセンターの設置地域が公開されているクラウドを利用する。 [追加策] 要求されるデータの機密性によっては、データセンターが適切な地域（たとえば国内）に設置されているクラウドを利用する。	Yes
				セキュリティ(全般)	L	1	セキュリティポリシ	サービスの運用に関わるセキュリティポリシをユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法（ウェブページに掲載、契約時に書面で交付など）を記述回答欄に記入してください。	サービスの運用に関わるセキュリティポリシが、カスタマに文書として開示されているクラウドを利用する。	Yes
				第三者認証	S	3	セキュリティ	当該のサービスに携わる部署は、セキュリティに関する第三者認証など（プライバシーマーク、ISO 27001、ISO 27017、ISO 27018など）を取得しているか「Yes/No」欄を選択してください。 「Yes」の場合、取得している第三者認証を記述回答欄に記入してください。（書き方ガイド「記入対象となる第三者認証」参照。）	プライバシーマーク、ISO 27001、ISO 27017、ISO 27018、あるいはそれらに準ずる第三者認証を取得しているクラウドを利用する。	Yes

		61	D2101-61 （外部委託に係る契約）（政府機関統一基準の対応項番 4.1.1(2))(p.60) 第六十一条 部局技術責任者又は職場情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。 一 委託先に提供する情報の委託先における目的外利用の禁止 二 委託先における情報セキュリティ対策の実施内容及び管理体制 三 委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制 四 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供 五 情報セキュリティインシデントへの対処方法 六 情報セキュリティ対策その他の契約の履行状況の確認方法 七 情報セキュリティ対策の履行が不十分な場合の対処方法 2 部局技術責任者又は職場情報セキュリティ責任者は、委託する業務において取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含めること。 一 情報セキュリティ監査の受入れ 二 サービスレベルの保証 3 部局技術責任者又は職場情報セキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、第一項及び前項の措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本学に提供し、本学の承認を受けるよう、仕様内容に含めること。	信頼性	E	1	サービス稼働率の規定	サービス稼働率を数値(例. 99.9%)で規定しているか「Yes/No」欄を選択してください。 「Yes」の場合、その値を記述回答欄に記入してください。また、SLAに規定している場合には、その旨を記入してください。	サービス稼働率が、SLAあるいはSLOとして、カスタマが参照可能な文書で明記されているクラウドを利用する。	Yes
				データセンター	K	6	データセンターの設置地域	データセンターが設置されている地域やゾーン（同一地域内で冗長化されている独立したデータセンターに相当する単位）を公表していいるか「Yes/No」欄を選択してください。 「Yes」の場合、地域名やゾーン数を記述回答欄に記入してください。契約後のみ開示される場合はその旨を記入してください。また、国内にデータセンターが設置されている場合(あるいは設置されていることを公表可能な場合)は、その旨を記入してください。	データセンターの設置地域が公開されているクラウドを利用する。 [追加策] 要求されるデータの機密性によっては、データセンターが適切な地域(たとえば国内) に設置されているクラウドを利用する。	Yes
				セキュリティ(全般)	L	1	セキュリティポリシ	サービスの運用に関わるセキュリティポリシをユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法（ウェブページに掲載、契約時に書面で交付など）を記述回答欄に記入してください。	サービスの運用に関わるセキュリティポリシが、カスタマに文書として開示されているクラウドを利用する。	Yes
				セキュリティ(全般)	L	3	インシデント対応（クラウド事業者管理のリソース）	クラウド事業者がサービスを提供するために用いるリソースにセキュリティインシデント（不正侵入、DoS攻撃、情報漏えいなど）が発生した場合の、事業者としての対応方針・方法をユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、ユーザが対応方針・方法を確認する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	インシデント発生時の対応方針や方法が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes
				セキュリティ(全般)	L	4	インシデント対応（ユーザ管理のリソース）	ユーザが管理しているリソースにセキュリティインシデント（不正侵入、DoS攻撃、情報漏えいなど）が発生した場合の、事業者としての対応方針・方法をユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、対応方針・方法（何もしない、ユーザに対応を依頼、サービス強制停止など）を記述回答欄に記入してください。また、対応がオプションサービスとなる場合はその旨を記入してください。	インシデント発生時の対応方針や方法が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes
				クラウド事業者の信頼性	O	1	経営状況	株式上場は行っているか「Yes/No」欄を選択してください。 「Yes」の場合、市場名も記述回答欄に記入してください。親会社が上場している場合はそちらについても記入してください。	サービスを提供する企業あるいはその親会社が株式上場等によって経営状況を開示しているクラウド、あるいは公的機関が提供するクラウドを極力利用する。	Yes
				クラウド事業者の信頼性	O	2	プライバシポリシ	サービスの提供・運用に関わるプライバシポリシをユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法（ウェブページに掲載、契約時に書面で交付など）を記述回答欄に記入してください。	サービスの提供・運用に関わるプライバシポリシが、契約書や約款等のカスタマが参照可能な文書で定められているクラウドを利用する。	Yes
				クラウド事業者の信頼性	O	3	第三者委託	サービスの実施について第三者への委託を行っているか「Yes/No」欄を選択してください。 「Yes」の場合、委託先での法令や各種ポリシ順守について文書で定められているか記述回答欄に記入してください。定められている場合、契約大学・研究機関がその文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記入してください。	第三者委託を行っている場合、委託先での法令や各種ポリシ順守について文書で定められており、カスタマにその事実が開示されているクラウドを利用する。	Yes/No
				クラウド事業者の信頼性	O	4	ユーザによる監査	ユーザ自身の認証取得のため、ユーザがサービスを監査することは可能か「Yes/No」欄を選択してください。 「Yes」の場合、何の監査が可能か記述回答欄に記入してください。	カスタマによる監査を受け入れるか、それが不可能でも第三者による監査結果がカスタマに開示可能であるクラウドを利用する。	Yes/No
				データの取り扱い	Q	1	データの知的財産権／使用権	ユーザがクラウドに格納したデータの知的財産権や使用権がクラウド事業者側には生じないことが契約書や約款等に明記されているか「Yes/No」欄を選択してください。 「Yes」の場合、契約大学・研究機関が文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	カスタマがクラウドに格納したデータの知的財産権や使用権がクラウド事業者側には生じないことが契約書や約款等に明記されているクラウドを利用する。	Yes

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

63	D2101-63（外部委託における対策の実施）（政府機関統一基準の対応項番4.1.1(3)）(p.64) 第六十三条 部局技術責任者又は職場情報セキュリティ責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認すること。 2 部局技術責任者又は職場情報セキュリティ責任者は、委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を利用者等より受けた場合は、委託事業を一時中断するなどの必要な措置を講じた上で、契約に基づく必要な措置を講じさせること。 3 部局技術責任者又は職場情報セキュリティ責任者は、委託した業務の終了時に、委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認すること。	セキュリティ(全般)	L	3	インシデント対応（クラウド事業者管理のリソース）	クラウド事業者がサービスを提供するために用いるリソースにセキュリティインシデント（不正侵入、DoS攻撃、情報漏えいなど）が発生した場合の、事業者としての対応方針・方法をユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、ユーザが対応方針・方法を確認する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	インシデント発生時の対応方針や方法が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes
		セキュリティ(全般)	L	4	インシデント対応（ユーザ管理のリソース）	ユーザが管理しているリソースにセキュリティインシデント（不正侵入、DoS攻撃、情報漏えいなど）が発生した場合の、事業者としての対応方針・方法をユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、対応方針・方法（何もしない、ユーザに対応を依頼、サービス強制停止など）を記述回答欄に記入してください。また、対応がオプションサービスとなる場合はその旨を記入してください。	インシデント発生時の対応方針や方法が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes
		クラウド事業者の信頼性	O	4	ユーザによる監査	ユーザ自身の認証取得のため、ユーザがサービスを監査することは可能か「Yes/No」欄を選択してください。 「Yes」の場合、何の監査が可能か記述回答欄に記入してください。	カスタマによる監査を受け入れるか、それが不可能でも第三者による監査結果がカスタマに開示可能であるクラウドを利用する。	Yes/No
		データの取り扱い	Q	2	データの削除	ユーザがデータを明に削除した時の当該データ、あるいはユーザの都合により契約を終了した後のユーザ情報およびユーザが所有していた全データが再利用されないことが保証されているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください（例：NIST-SP-800-88に準拠した方法でデータをすべて削除する、など）。削除証明書の発行が可能な場合には記入してください。	カスタマによるデータ削除時の当該データやカスタマの契約終了後のカスタマ情報およびカスタマ所有データが、復元不可能な方法で削除されることが保証されるクラウドを利用する（データの削除証明書を発行してくれるクラウド事業者もある）。 [利用側の施策] カスタマがデータの削除を行う場合は、クラウド事業者から提示された当該データを復元不可能とする削除方法に従って削除を実施する。	Yes
64	D2101-64（外部委託における情報の取扱い）（政府機関統一基準の対応項番4.1.1(4)）(p.64) 第六十四条 利用者等は、委託先への情報の提供等において、以下の事項を遵守すること。 一 委託先に要保護情報を提供する場合、提供する情報を必要最小限とし、あらかじめ定めら れた安全な受渡し方法により提供すること。 二 提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は抹消させること。 三 委託業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかに部局技術責任者又は職場情報セキュリティ責任者に報告すること。	セキュリティ(全般)	L	3	インシデント対応（クラウド事業者管理のリソース）	クラウド事業者がサービスを提供するために用いるリソースにセキュリティインシデント（不正侵入、DoS攻撃、情報漏えいなど）が発生した場合の、事業者としての対応方針・方法をユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、ユーザが対応方針・方法を確認する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	インシデント発生時の対応方針や方法が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes
		セキュリティ(全般)	L	4	インシデント対応（ユーザ管理のリソース）	ユーザが管理しているリソースにセキュリティインシデント（不正侵入、DoS攻撃、情報漏えいなど）が発生した場合の、事業者としての対応方針・方法をユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、対応方針・方法（何もしない、ユーザに対応を依頼、サービス強制停止など）を記述回答欄に記入してください。また、対応がオプションサービスとなる場合はその旨を記入してください。	インシデント発生時の対応方針や方法が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes
		データの取り扱い	Q	2	データの削除	ユーザがデータを明に削除した時の当該データ、あるいはユーザの都合により契約を終了した後のユーザ情報およびユーザが所有していた全データが再利用されないことが保証されているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください（例：NIST-SP-800-88に準拠した方法でデータをすべて削除する、など）。削除証明書の発行が可能な場合には記入してください。	カスタマによるデータ削除時の当該データやカスタマの契約終了後のカスタマ情報およびカスタマ所有データが、復元不可能な方法で削除されることが保証されるクラウドを利用する（データの削除証明書を発行してくれるクラウド事業者もある）。 [利用側の施策] カスタマがデータの削除を行う場合は、クラウド事業者から提示された当該データを復元不可能とする削除方法に従って削除を実施する。	Yes

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

第二節 約款による外部サービスの利用	66	D2101-66（約款による外部サービスの利用に係る対策）（ 政府機関統一基準の対応項番4.1.2(1)-1）(p.68) 第六十六条 全学実施責任者は、本学において約款による外部サービスを業務に利用する場合は、以下を例に利用手続及び運用手順を定めること。 三 サービス利用中の安全管理に係る運用手順 ・サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認 ・情報の滅失、破壊等に備えたバックアップの取得 ・利用者への定期的な注意喚起（禁止されている要機密情報の取扱いの有無の確認等）	データ管理	M	2	ログの使用権（閲覧等）	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の使用権（閲覧等）がユーザ（または契約大学・研究機関）に認められているか「Yes/No」欄を選択してください。 「Yes」の場合、閲覧できるログの種類を記述回答欄に記入してください。さらに閲覧するログをユーザがダウンロードして保管することが可能であれば記入してください。	必要なログを取得するために、利用するクラウドのログの使用権（閲覧等）が認められているクラウドを利用する。 [追加策/要件に応じて検討] 利用するクラウドの時刻設定が可能な場合には、タイムサーバなどを利用して基準となる時刻に同期させる。また、ログに時刻情報も記録されるように設定する。 データにアクセスした利用者を特定できるようなアクセスログを取得できるように設定する。 データベースの操作ログを取得できるように設定する。 VPN回線を利用してクラウドを利用する場合、主体認証ログを取得できるように設定し管理する。	Yes
			バックアップ	N	1	バックアップサービスの有無	ユーザがクラウドに格納したデータあるいはユーザが作成したサーバイメージのバックアップを行うサービスは提供されているか「Yes/No」欄を選択してください。（管理者権限をもったユーザのスクリプト等による実現は除く）。	バックアップサービスを提供しているクラウドの場合はその機能を利用する。 提供していないクラウドの場合は、利用者側でバックアップを取得する。	Yes/No
	67	D2101-67（約款による外部サービスの利用における対策の実施）（政府機関統一基準の対応項番 4.1.2(2)）(p.69) 第六十七条 利用者等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用すること。	契約申込み	C	1	契約書の有無・その他の交付書面の種類	契約内容を明記する書面はあるか「Yes/No」欄を選択してください。Yesの場合は、その種類（契約書・約款等）と言語を記述回答欄に記入してください。（例：契約書（日本語）、サービス利用規約（英語）、など）	契約書あるいは約款などの形で契約内容・条件が明記された文書がカスタマに提供されるクラウドを利用する。	Yes
			信頼性	E	1	サービス稼働率の規定	サービス稼働率を数値(例. 99.9%)で規定しているか 「Yes/No」欄を選択してください。 「Yes」の場合、その値を記述回答欄に記入してください。 また、SLAに規定している場合には、その旨を記入してください。	サービス稼働率が、SLAあるいはSLOとして、カスタマが参照可能な文書で明記されているクラウドを利用する。	Yes
			セキュリティ(全般)	L	8	セキュリティ対策	ウイルス検知・防御のサービスが提供されているか 「Yes/No」欄を選択してください（IaaS等でユーザが独自にソフトウェアを導入する場合を除く）。「Yes」の場合、基本サービスかオプションサービスかを記述回答欄に記入してください。	不正プログラム対策ソフトウェア(マルウェア検知・防御のサービスなど)が提供されているクラウドを利用し、当該サービスを使用する。 不正プログラム対策ソフトウェアが提供されていないクラウドの場合には、カスタマ側で不正プログラム対策ソフトウェアを導入するなどの対策を行った上で利用する。	Yes/No
			データ管理	M	6	データの多重化	ユーザが格納したデータは多重化されているか 「Yes/No」欄を選択してください。 「Yes」の場合、どのような手法か（RAID、複数データセンターに保存など）記述回答欄に記入してください。災害対応など冗長性を考慮しているか記入してください。	格納データがデータセンタ内で多重化されているサービスを利用する。 [追加策] 必要に応じて、データセンタ間で多重化されている（あるいは多重化可能な）クラウドを利用する。	Yes
			契約条件	P	2	契約条件・SLAの変更手続き	契約期間中に、クラウド事業者が契約条件やSLAの変更を行う場合の手続きが文書で定められているか 「Yes/No」欄を選択してください。 「Yes」の場合、契約大学・研究機関がその文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	契約条件やSLAの変更手続きが、契約書や約款等のカスタマが参照可能な文書で定められているクラウドを利用する。	Yes
			データの取り扱い	Q	2	データの削除	ユーザがデータを明に削除した時の当該データ、あるいはユーザの都合により契約を終了した後のユーザ情報およびユーザが所有していた全データが再利用されないことが保証されているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください（例：NIST-SP-800-88に準拠した方法でデータをすべて削除する、など）。削除証明書の発行が可能な場合には記入してください。	カスタマによるデータ削除時の当該データやカスタマの契約終了後のカスタマ情報およびカスタマ所有データが、復元不可能な方法で削除されることが保証されるクラウドを利用する（データの削除証明書を発行してくれるクラウド事業者もある）。 [利用側の施策] カスタマがデータの削除を行う場合は、クラウド事業者から提示された当該データを復元不可能とする削除方法に従って削除を実施する。	Yes
第四節 クラウドサービスの利用	70	D2101-70（クラウドサービスの利用における対策）（政府機関統一基準の対応項番4.1.4(1)）(p.74) 第七十条 部局技術責任者は、クラウドサービス（民間事業者が提供するものに限らず、政府等が提供するものを含む。以下同じ。）を利用するに当たり、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断すること。 2 部局技術責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定すること。 3 部局技術責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件とすること。 4 部局技術責任者は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めること。	データセンター	K	6	データセンターの設置地域	データセンターが設置されている地域やゾーン（同一地域内で冗長化されている独立したデータセンターに相当する単位）を公表しているか「Yes/No」欄を選択してください。 「Yes」の場合、地域名やゾーン数を記述回答欄に記入してください。契約後のみ開示される場合はその旨を記入してください。また、国内にデータセンターが設置されている場合(あるいは設置されていることを公表可能な場合)は、その旨を記入してください。	データセンターの設置地域が公開されているクラウドを利用する。 [追加策] 要求されるデータの機密性によっては、データセンターが適切な地域（たとえば国内）に設置されているクラウドを利用する。	Yes

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

			5 部局技術責任者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断すること。	データセンター	K	7	地域・ゾーンの指定	どの地域・ゾーン（同一地域内で冗長化されている独立したデータセンターに相当する単位）にあるデータセンターを利用するか（ファイルの保存も含む）をユーザが指定することは可能か「Yes/No」欄を選択してください。	[要件に応じて検討] 要求されるデータの機密性に応じて、適切な地域・ゾーン（たとえば国内）に設置されているデータセンターを指定する。	Yes
				セキュリティ(全般)	L	2	ユーザが利用するリソースの分離	ユーザが利用するリソースは、他のユーザのリソースとどのレベルで分離されているか記述回答欄に記入してください（例：アプリケーション、VM、物理マシン）。	可能な限りリソースの分離方式が開示されているクラウドを利用する。 [利用側の施策] 以下のような分離レベルから生じるセキュリティリスクを理解して利用する。一般に、同一ハードウェア上でソフトウェアによって分離されているものは、当該ソフトウェアの脆弱性や他の利用者（テナント）からの攻撃によるリスクがないとは言えない。ハードウェアレベルで分離されていればこのようなリスクは軽減されるが、データセンターの内部ネットワークに対する攻撃などの可能性は残る。	記述回答に具体的な記述があるか、適切な情報源が示されている。
				バックアップ	N	6	バックアップデータのセキュリティ	バックアップデータのアクセス制限や暗号化に関して、元のデータと同等のセキュリティレベルが継承されているか「Yes/No」欄を選択してください。	バックアップデータに対して元データと同等のセキュリティレベルが実現されるクラウドを利用する。 [利用側の施策] 必要な場合はそれが可能となる設定や利用方法を実施する。	Yes
				クラウド事業者の信頼性	O	5	サービスの監査結果の開示	提供しているサービスが認証取得などのために外部監査を受けている場合、監査結果を開示しているか 「Yes/No」欄を選択してください。 「Yes」の場合、受けた外部監査の種類を記述回答欄に記入してください。	第三者による監査結果をカスタマに開示しているか、あるいは請求によって開示可能であるクラウドを利用する。	Yes
				クラウド事業者の信頼性	O	6	国内法人 / 国内総代理店等の有無	（海外に主たる拠点を置く事業者のみ回答）日本国内法人もしくは国内総代理店など、国内に営業やサポートの窓口となる組織を有しているか「Yes/No」欄を選択してください。	国内に営業やサポートの窓口となる組織を有しているクラウドを利用する。	Yes
				契約条件	P	1	責任範囲の明確化	クラウド事業者と大学（ないしエンドユーザ）の責任分界点は文書で定められているか「Yes/No」欄を選択してください。 「Yes」の場合、契約大学・研究機関がその文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	責任分界点が、契約書や約款等のカスタマが参照可能な文書で定められているクラウドを利用する。	Yes
				契約条件	P	4	準拠法	係争時の準拠法は日本法か「Yes/No」欄を選択してください。 「No」の場合、国・州名を記述回答欄に記入してください。	係争時の準拠法が日本法であるクラウドを利用する。	Yes
				契約条件	P	5	管轄裁判所	指定管轄裁判所はあるか「Yes/No」欄を選択してください。 「Yes」の場合、管轄裁判所を記述回答欄に記入してください。	指定管轄裁判所が日本国内の裁判所であるクラウドを利用する。	Yes
				契約条件	P	6	事業終了の告知時期	クラウド事業者が事業を終了する場合、何か月前に終了を告知されるかが契約書や約款などの文書に定められているか「Yes/No」欄を選択してください。 「Yes」の場合、契約大学・研究機関がその文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	事業終了の告知が、カスタマ側が対応するのに十分な時間的余裕をもって行われる(たとえば6か月以前)であることが、契約書や約款等のカスタマが参照可能な文書で定められているクラウドを利用する。	Yes
				リソースの引継ぎ	R	1	契約終了時のデータの移行支援	ユーザの都合により契約を終了した時、ユーザがデータ移行の支援を受けることは可能か「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください。	データ移行の支援が受けられるクラウドを利用するか、あるいはクラウドからのデータの取出し方法に関して一括ダウンロードコマンド等の機能およびドキュメンテーションが完備しているクラウドを利用する。	Yes/No
				リソースの引継ぎ	R	2	サービス利用終了時のデータ確保	ユーザの都合により契約を終了する時やクラウド事業者が事業を終了する時、サービス利用終了前にユーザがデータを完全な形で取り出す方法が担保されているか 「Yes/No」欄を選択してください。 「Yes」の場合、データの取得方法（ダウンロード、物理媒体の提供等）を記述回答欄に記入してください。	データ移行の支援が受けられるクラウド、あるいはクラウドからのデータの取出し方法に関して一括ダウンロードコマンド等の機能およびドキュメンテーションが完備しているクラウドを利用する。	Yes
				リソースの引継ぎ	R	3	サーバイメージの移行性	サーバイメージをオンプレミスの環境や他社クラウドにダウンロードして動作させることは可能か「Yes/No」欄を選択してください。 「Yes」の場合、条件・方法について記述回答欄に記入してください。	サーバイメージに関してオンプレミスの仮想環境や他社クラウドと互換性のあるクラウドを利用する。 [別案] 移行が必要となる可能性のあるアプリケーションに関しては、コンテナを利用する。	Yes/No

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

				リソースの引継ぎ	R	4	ユーザデータの移行性	オンプレミスの環境や他社クラウドにユーザデータを移行することが可能か「Yes/No」欄を選択してください。 「Yes」の場合、何らかの移行ツールや手段は提供されるか記述回答欄に記入してください。	データ移行の支援が受けられるクラウド、あるいはクラウドからのデータの取出し方法に関して一括ダウンロードコマンド等の機能およびドキュメンテーションが完備しているクラウドを利用する。	Yes
				第三者認証	S	3	セキュリティ	当該のサービスに携わる部署は、セキュリティに関する第三者認証など（プライバシーマーク、ISO 27001、ISO 27017、ISO 27018など）を取得しているか「Yes/No」欄を選択してください。 「Yes」の場合、取得している第三者認証を記述回答欄に記入してください。（書き方ガイド「記入対象となる第三者認証」参照。）	プライバシーマーク、ISO 27001、ISO 27017、ISO 27018、あるいはそれらに準ずる第三者認証を取得しているクラウドを利用する。	Yes
				第三者認証	S	4	経営・事業	経営・事業に関する第三者認証（SOC1、ISO 14001など）を取得しているか「Yes/No」欄を選択してください。 「Yes」の場合、取得している第三者認証を記述回答欄に記入してください。（書き方ガイド「記入対象となる第三者認証」参照。）	SOC1、ISO 14001、あるいはそれらに準ずる第三者認証を取得しているクラウドを利用する。	Yes
		71	D2101-71（クラウドサービスの中断や終了時の業務移行に係る対策）（政府機関統一基準の対応項番 4.1.4(1)-1,2）(p.78) 第七十一条 部局技術責任者は、クラウドサービスを利用するに当たり、サービスの中断や終了時に際し、円滑に業務を移行するための対策として、以下を例とするセキュリティ対策を実施することをクラウドサービスの選定条件とし、仕様内容にも含めること。 一 取り扱う情報の可用性区分の格付に応じた、サービス中断時の復旧要件 二 取り扱う情報の可用性区分の格付に応じた、サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法 2 部局技術責任者は、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティ対策を構築すること。また、対策を実現するために、以下を例とするセキュリティ要件をクラウドサービスに求め、契約内容にも含めること。特に、運用段階で委託先が変更となる場合、開発段階等で設計したクラウドサービスのセキュリティ要件のうち継承が必須なセキュリティ要件について、変更後の委託先における維持・向上の確実性を事前に確認すること。 一 クラウドサービスに係るアクセスログ等の証跡の保存及び提供 二 インターネット回線とクラウド基盤の接続点の通信の監視 三 クラウドサービスの委託先による情報の管理・保管の実施内容の確認 四 クラウドサービス上の脆弱性対策の実施内容の確認 五 クラウドサービス上の情報に係る復旧時点目標(RPO)等の指標 六 クラウドサービス上で取り扱う情報の暗号化 七 利用者の意思によるクラウドサービス上で取り扱う情報の確実な削除・廃棄 八 利用者が求める情報開示請求に対する開示項目や範囲の明記	信頼性	E	1	サービス稼働率の規定	サービス稼働率を数値(例. 99.9%)で規定しているか 「Yes/No」欄を選択してください。 「Yes」の場合、その値を記述回答欄に記入してください。 また、SLAに規定している場合には、その旨を記入してください。	サービス稼働率が、SLAあるいはSLOとして、カスタマが参照可能な文書で明記されているクラウドを利用する。	Yes
				信頼性	E	4	計画停止の有無	ユーザに影響を与える計画停止があるか「Yes/No」欄を選択してください。 「Yes」の場合、頻度および標準的な停止時間（例：〇時から〇時まで完全停止、〇時から〇時の間で5分程度停止など）を記述回答欄に記入してください。ここで、計画停止とは月次等の定期的なメンテナンスや法定停電による停止などのことです。	計画停止がないか(無停止保守を実現)、計画停止がある場合はその頻度・時間が明示され、事前にカスタマに通知されるクラウドを利用する。	Yes
				サポート関連	F	2	重要情報の通知	サービス停止、障害、保守実施、非互換を伴う仕様変更などの通知手順が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法（ウェブページに掲載（可能ならばURLを記入）、電子メール、契約時に書面で交付など）を記述回答欄に記入してください。	サービス停止、障害、保守実施、非互換を伴う仕様変更などの通知手順が、カスタマが参照可能な文書で定められている手順に従って事前に行われるクラウドを利用する。	Yes
				ネットワーク・通信機能	G	2	通信のセキュリティ確保	端末からサーバまでの通信のセキュリティ確保がサービスとして提供されているか「Yes/No」欄を選択してください。 「Yes」の場合、どのようにセキュリティを確保しているか、方式（SSHやSSL/TLSによる暗号化、ファイル共有におけるAES、SINET L2VPN、IPsec、SSL-VPN等）を記述回答欄に記入してください。	端末からサーバまでの通信に関して、「電子政府推奨暗号リスト」に記載された複数の暗号化アルゴリズムおよびそれに基づいた安全なプロトコルを選択することが可能なクラウドを利用する。 [追加策] VPN回線でクラウドを利用する場合、二重の暗号化を行う（例えば、インターネット VPN 回線において IPsec で通信経路の暗号化を行った上で HTTPS 通信によりコンテンツの暗号化を行 う)などを考慮する。	Yes
				セキュリティ(全般)	L	1	セキュリティポリシ	サービスの運用に関わるセキュリティポリシをユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法（ウェブページに掲載、契約時に書面で交付など）を記述回答欄に記入してください。	サービスの運用に関わるセキュリティポリシが、カスタマに文書として開示されているクラウドを利用する。	Yes
				セキュリティ(全般)	L	5	バージョンアップの頻度	クラウド事業者がサービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、その頻度あるいは基準を記述回答欄に記入してください。	サービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes
				セキュリティ(全般)	L	8	セキュリティ対策	ウイルス検知・防御のサービスが提供されているか 「Yes/No」欄を選択してください（IaaS等でユーザが独自にソフトウェアを導入する場合を除く）。「Yes」の場合、基本サービスかオプションサービスかを記述回答欄に記入してください。	不正プログラム対策ソフトウェア(マルウェア検知・防御のサービスなど)が提供されているクラウドを利用し、当該サービスを使用する。 不正プログラム対策ソフトウェアが提供されていないクラウドの場合には、カスタマ側で不正プログラム対策ソフトウェアを導入するなどの対策を行った上で利用する。	Yes/No

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

				データ管理	M	1	ログの知的財産権	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の知的財産権がクラウド事業者とユーザ（または契約大学）のいずれに帰属するか、契約書や約款等に明記されているか「Yes/No」欄を選択してください。 「Yes」の場合、契約大学・研究機関が文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	必要なログを取得するために、ログの知的財産権が利用者に帰属するクラウドを利用する。	Yes
				データ管理	M	2	ログの使用権（閲覧等）	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の使用権（閲覧等）がユーザ（または契約大学・研究機関）に認められているか「Yes/No」欄を選択してください。 「Yes」の場合、閲覧できるログの種類を記述回答欄に記入してください。さらに閲覧するログをユーザがダウンロードして保管することが可能であれば記入してください。	必要なログを取得するために、利用するクラウドのログの使用権（閲覧等）が認められているクラウドを利用する。 [追加策/要件に応じて検討] 利用するクラウドの時刻設定が可能な場合には、タイムサーバなどを利用して基準となる時刻に同期させる。また、ログに時刻情報も記録されるように設定する。 データにアクセスした利用者を特定できるようなアクセスログを取得できるように設定する。 データベースの操作ログを取得できるように設定する。 VPN回線を利用してクラウドを利用する場合、主体認証ログを取得できるように設定し管理する。	Yes
				データ管理	M	3	ログの使用（閲覧等）可能期間	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の使用（閲覧等）の可能期間が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、可能期間を記述回答欄に記入してください。また、大学・研究機関からの要請により、可能期間を延長または短縮することが可能な場合には、記入してください。	[利用側の施策] 利用するクラウドのログの使用（閲覧等）の可能期間を確認し、大学等で定めたログの保存期間中はログを管理できるようにする。サービスにおけるログの使用可能期間が大学等で定めた保存期間より短い場合には、ログをログサーバ等に保管し、定めたログの保存期間中はログを閲覧できるようにする。	Yes/No
				データ管理	M	4	データの暗号化	保存するユーザのデータは暗号化が可能か「Yes/No」欄を選択してください。 「Yes」の場合、暗号化する方式を記述回答欄に記入してください（ユーザが暗号化の要否を選択する、システムが自動で暗号化するなど）。	トランザクションデータおよび保存データの両方に関して「電子政府推奨暗号リスト」に記載された複数の暗号化アルゴリズムおよびそれに基づいた安全なプロトコルを選択することが可能なクラウドを利用する。	Yes
				クラウド事業者の信頼性	O	2	プライバシポリシ	サービスの提供・運用に関わるプライバシポリシをユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法（ウェブページに掲載、契約時に書面で交付など）を記述回答欄に記入してください。	サービスの提供・運用に関わるプライバシポリシが、契約書や約款等のカスタマが参照可能な文書で定められているクラウドを利用する。	Yes
				クラウド事業者の信頼性	O	4	ユーザによる監査	ユーザ自身の認証取得のため、ユーザがサービスを監査することは可能か「Yes/No」欄を選択してください。 「Yes」の場合、何の監査が可能か記述回答欄に記入してください。	カスタマによる監査を受け入れるか、それが不可能でも第三者による監査結果がカスタマに開示可能であるクラウドを利用する。	Yes/No
				契約条件	P	2	契約条件・SLAの変更手続き	契約期間中に、クラウド事業者が契約条件やSLAの変更を行う場合の手続きが文書で定められているか 「Yes/No」欄を選択してください。 「Yes」の場合、契約大学・研究機関がその文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	契約条件やSLAの変更手続きが、契約書や約款等のカスタマが参照可能な文書で定められているクラウドを利用する。	Yes
				契約条件	P	6	事業終了の告知時期	クラウド事業者が事業を終了する場合、何か月前に終了を告知されるかが契約書や約款などの文書に定められているか「Yes/No」欄を選択してください。 「Yes」の場合、契約大学・研究機関がその文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	事業終了の告知が、カスタマ側が対応するのに十分な時間的余裕をもって行われる(たとえば6か月以前)であることが、契約書や約款等のカスタマが参照可能な文書で定められているクラウドを利用する。	Yes
				データの取り扱い	Q	2	データの削除	ユーザがデータを明に削除した時の当該データ、あるいはユーザの都合により契約を終了した後のユーザ情報およびユーザが所有していた全データが再利用されないことが保証されているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください（例：NIST-SP-800-88に準拠した方法でデータをすべて削除する、など）。削除証明書の発行が可能な場合には記入してください。	カスタマによるデータ削除時の当該データやカスタマの契約終了後のカスタマ情報およびカスタマ所有データが、復元不可能な方法で削除されることが保証されるクラウドを利用する（データの削除証明書を発行してくれるクラウド事業者もある）。 [利用側の施策] カスタマがデータの削除を行う場合は、クラウド事業者から提示された当該データを復元不可能とする削除方法に従って削除を実施する。	Yes

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

				リソースの引継ぎ	R	1	契約終了時のデータの移行支援	ユーザの都合により契約を終了した時、ユーザがデータ移行の支援を受けることは可能か「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください。	データ移行の支援が受けられるクラウドを利用するか、あるいはクラウドからのデータの取出し方法に関して一括ダウンロードコマンド等の機能およびドキュメンテーションが完備しているクラウドを利用する。	Yes/No
				リソースの引継ぎ	R	2	サービス利用終了時のデータ確保	ユーザの都合により契約を終了する時やクラウド事業者が事業を終了する時、サービス利用終了前にユーザがデータを完全な形で取り出す方法が担保されているか	データ移行の支援が受けられるクラウド、あるいはクラウドからのデータの取出し方法に関して一括ダウンロードコマンド等の機能およびドキュメンテーションが完備しているクラウドを利用する。	Yes
				リソースの引継ぎ	R	3	サーバイメージの移行性	サーバイメージをオンプレミスの環境や他社クラウドにダウンロードして動作させることは可能か「Yes/No」欄を選択してください。 「Yes」の場合、条件・方法について記述回答欄に記入してください。	サーバイメージに関してオンプレミスの仮想環境や他社クラウドと互換性のあるクラウドを利用する。 [別案] 移行が必要となる可能性のあるアプリケーションに関しては、コンテナを利用する。	Yes/No
				リソースの引継ぎ	R	4	ユーザデータの移行性	オンプレミスの環境や他社クラウドにユーザデータを移行することが可能か「Yes/No」欄を選択してください。 「Yes」の場合、何らかの移行ツールや手段は提供されるか記述回答欄に記入してください。	データ移行の支援が受けられるクラウド、あるいはクラウドからのデータの取出し方法に関して一括ダウンロードコマンド等の機能およびドキュメンテーションが完備しているクラウドを利用する。	Yes
第八章 情報システムに係る文書等の整備	第二節 機器等の調達に係る規定の整備	76	D2101-76（機器等の調達に係る規定の整備）（政府機関統一基準の対応項番5.1.2(1)）(p.85) 第七十六条 全学実施責任者は、機器等の選定基準を整備すること。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を本学が確認できることを加えること。	サポート関連	F	1	サポート窓口	サポートについて、記述回答欄に以下を記入してください。サポートプラン（有償・無償など）毎に異なる場合はそれぞれについて記入してください。 ・窓口（例：メール、電話、チャット、など） ・受付時間帯（例：平日 9:00-17:00、24時間365日、など） ・回答時間（例：無償の標準プランの場合は1営業日以内、有償の〇〇プランの場合は4時間以内、など） ・対応言語（例：日本語のみ、日本語と英語、など）	サポートレベルに関する具体的な条件が契約書や約款等のカスタマが参照可能な文書で定められているクラウドを利用する。	記述回答に具体的な記述があるか、適切な情報源が示されている。
				第三者認証	S	3	セキュリティ	当該のサービスに携わる部署は、セキュリティに関する第三者認証など（プライバシーマーク、ISO 27001、ISO 27017、ISO 27018など）を取得しているか「Yes/No」欄を選択してください。 「Yes」の場合、取得している第三者認証を記述回答欄に記入してください。（書き方ガイド「記入対象となる第三者認証」参照。）	プライバシーマーク、ISO 27001、ISO 27017、ISO 27018、あるいはそれらに準ずる第三者認証を取得しているクラウドを利用する。	Yes
				第三者認証	S	4	経営・事業	経営・事業に関する第三者認証（SOC1、ISO 14001など）を取得しているか「Yes/No」欄を選択してください。 「Yes」の場合、取得している第三者認証を記述回答欄に記入してください。（書き方ガイド「記入対象となる第三者認証」参照。）	SOC1、ISO 14001、あるいはそれらに準ずる第三者認証を取得しているクラウドを利用する。	Yes
第九章 情報システムのライフサイクルの各段階における対策	第一節 情報システムの企画・要件定義	81	D2101-81（情報システムのセキュリティ要件に係る対策）（政府機関統一基準の対応項番5.2.1(2)-1,2,3,4,5）(p.92) 第八十一条 5 部局技術責任者は、開発する情報システムに関連する脆弱性への対策が実施されるよう、以下を含む対策を仕様書等に明記すること。 三 セキュリティ侵害につながる脆弱性が情報システムに存在することが発覚した場合に修正が施されること。	セキュリティ(全般)	L	5	バージョンアップの頻度	クラウド事業者がサービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、その頻度あるいは基準を記述回答欄に記入してください。	サービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes
				セキュリティ(全般)	L	6	アップデート情報（脆弱性情報）の提供	サーバのメニュー、テンプレート、イメージとして提供されているOS・アプリケーション等のアップデート情報や脆弱性情報はユーザに提供されるか「Yes/No」欄を選択してください。	サービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準がカスタマに文書として開示されているクラウドを利用する。 [追加策] 利用しているサーバに対して可能な範囲で脆弱性診断を実施することを検討する。	Yes
		87	D2101-87（情報システムの運用・保守を外部委託する場合の対策）（政府機関統一基準の対応項番 5.2.1(4)-1）(p.98) 第八十七条 部局技術責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるために、以下を含む要件を調達仕様書に記載するなどして、適切に実施させること。	セキュリティ(全般)	L	1	セキュリティポリシ	サービスの運用に関わるセキュリティポリシをユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法（ウェブページに掲載、契約時に書面で交付など）を記述回答欄に記入してください。	サービスの運用に関わるセキュリティポリシが、カスタマに文書として開示されているクラウドを利用する。	Yes

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

			一 情報システムの運用環境に課せられるべき条件の整備 二 情報システムのセキュリティ監視を行う場合の監視手順や連絡方法 三 情報システムの保守における情報セキュリティ対策 四 運用中の情報システムに脆弱性が存在することが判明した場合の情報セキュリティ対策	セキュリティ(全般)	L	3	インシデント対応（クラウド事業者管理のリソース）	クラウド事業者がサービスを提供するために用いるリソースにセキュリティインシデント（不正侵入、DoS攻撃、情報漏えいなど）が発生した場合の、事業者としての対応方針・方法をユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、ユーザが対応方針・方法を確認する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	インシデント発生時の対応方針や方法が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes
				セキュリティ(全般)	L	4	インシデント対応（ユーザ管理のリソース）	ユーザが管理しているリソースにセキュリティインシデント（不正侵入、DoS攻撃、情報漏えいなど）が発生した場合の、事業者としての対応方針・方法をユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、対応方針・方法（何もしない、ユーザに対応を依頼、サービス強制停止など）を記述回答欄に記入してください。また、対応がオプションサービスとなる場合はその旨を記入してください。	インシデント発生時の対応方針や方法が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes
				セキュリティ(全般)	L	5	バージョンアップの頻度	クラウド事業者がサービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、その頻度あるいは基準を記述回答欄に記入してください。	サービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes
	第三節 情報システムの運用・保守	92	D2101-92（情報システムの運用・保守時の対策）（政府機関統一基準の対応項番5.2.3(1)）(p.101) 第九十二条 部局技術責任者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用すること。 2 部局技術責任者は、基盤となる情報システムを利用して構築された情報システムを運用する場合は、基盤となる情報システムを整備し、運用管理する本学との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用すること。 3 部局技術責任者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。	データ管理	M	2	ログの使用権（閲覧等）	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の使用権（閲覧等）がユーザ（または契約大学・研究機関）に認められているか「Yes/No」欄を選択してください。 「Yes」の場合、閲覧できるログの種類を記述回答欄に記入してください。さらに閲覧するログをユーザがダウンロードして保管することが可能であれば記入してください。	必要なログを取得するために、利用するクラウドのログの使用権（閲覧等）が認められているクラウドを利用する。 [追加策/要件に応じて検討] 利用するクラウドの時刻設定が可能な場合には、タイムサーバなどを利用して基準となる時刻に同期させる。また、ログに時刻情報も記録されるように設定する。 データにアクセスした利用者を特定できるようなアクセスログを取得できるように設定する。 データベースの操作ログを取得できるように設定する。 VPN回線を利用してクラウドを利用する場合、主体認証ログを取得できるように設定し管理する。	Yes
				契約条件	P	1	責任範囲の明確化	クラウド事業者と大学（ないしエンドユーザ）の責任分界点は文書で定められているか「Yes/No」欄を選択してください。 「Yes」の場合、契約大学・研究機関がその文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	責任分界点が、契約書や約款等のカスタマが参照可能な文書で定められているクラウドを利用する。	Yes
		93	D2101-93（情報システムの運用・保守時の対策事項）（ 政府機関統一基準の対応項番5.2.3(1)-1,2,3,4）(p.101) 第九十三条 部局技術責任者は、情報システムのセキュリティ監視を行う場合は、以下の内容を含む監視手順を定め、適切に監視運用すること。 一 監視するイベントの種類 二 監視体制 三 監視状況の報告手順 四 情報セキュリティインシデントを認知した場合の報告手順 五 監視運用における情報の取扱い（機密性の確保） 2 部局技術責任者は、情報システムに実装されたセキュリティ機能が適切に運用されていることを確認すること。 4 部局技術責任者は、運用中の情報システムの脆弱性の存在が明らかになった場合には、情報セキュリティを確保するための措置を講ずること。	管理機能	H	2	稼働状況の一覧表示機能	ユーザに割り当てられたプロセスの死活やリソースの使用率などのサービス稼働状況を一覧で表示する機能は提供されるか「Yes/No」欄を選択してください。	サービス稼働状況やネットワーク状況を確認できる機能が提供されているクラウドを利用する。 [利用側の施策] その機能を使用して運用状況を確認・記録し、それに基づいてサーバやネットワークの資源を適切に分配・管理する。	Yes
				管理機能	H	9	プロセス監視機能	ユーザに割り当てられたプロセスの死活やリソースの使用率の監視・アラート機能は提供されるか「Yes/No」欄を選択してください。	プロセスの監視・アラート機能が提供されているクラウドを利用する。 [利用側の施策] 当機能によって状況を確認し、サーバやネットワークの資源を適切に分配・管理する。	Yes
				セキュリティ(全般)	L	3	インシデント対応（クラウド事業者管理のリソース）	クラウド事業者がサービスを提供するために用いるリソースにセキュリティインシデント（不正侵入、DoS攻撃、情報漏えいなど）が発生した場合の、事業者としての対応方針・方法をユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、ユーザが対応方針・方法を確認する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	インシデント発生時の対応方針や方法が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes
				セキュリティ(全般)	L	5	バージョンアップの頻度	クラウド事業者がサービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、その頻度あるいは基準を記述回答欄に記入してください。	サービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

				セキュリティ(全般)	L	6	アップデート情報（脆弱性情報）の提供	サーバのメニュー、テンプレート、イメージとして提供されているOS・アプリケーション等のアップデート情報や脆弱性情報はユーザに提供されるか「Yes/No」欄を選択してください。	サービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準がカスタマに文書として開示されているクラウドを利用する。 [追加策] 利用しているサーバに対して可能な範囲で脆弱性診断を実施することを検討する。	Yes
				セキュリティ(全般)	L	10	ログ分析・脅威検出	ログ分析やセキュリティ上の脅威の自動検出を行う機能（SIEM(Security Information and Event Management)、CASB(Cloud Access Security Broker)等）が提供されるか「Yes/No」欄を選択してください。 「Yes」の場合、具体的な機能を記述回答欄に記入してください。	[要件に応じて検討] 内部および外部からの不正アクセスのチェック・分析の頻度や分析の精度を高める必要がある場合、専任の分析担当者の設置、ログ分析やセキュリティ上の脅威の自動検出を行う機能の利用、監視事業者への委託(F4, F5)を検討する 。	Yes/No
				セキュリティ(全般)	L	11	IDS・IPS	IDS（不正侵入検知システム）・IPS（不正侵入予防システム）はサービスとして提供されているか「Yes/No」欄を選択してください。	[要件に応じて検討] 必要に応じて、IDS（不正侵入検知システム）/IPS（不正侵入予防システム）が提供されているクラウドを利用し、当該機能を使用する。 IPS/IDSが提供されていないクラウドの場合には、カスタマ側でこれらのシステムを導入するなどの対策を行った上で利用する。	Yes/No
				データ管理	M	2	ログの使用権（閲覧等）	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の使用権（閲覧等）がユーザ（または契約大学・研究機関）に認められているか「Yes/No」欄を選択してください。 「Yes」の場合、閲覧できるログの種類を記述回答欄に記入してください。さらに閲覧するログをユーザがダウンロードして保管することが可能であれば記入してください。	必要なログを取得するために、利用するクラウドのログの使用権（閲覧等）が認められているクラウドを利用する。 [追加策/要件に応じて検討] 利用するクラウドの時刻設定が可能な場合には、タイムサーバなどを利用して基準となる時刻に同期させる。また、ログに時刻情報も記録されるように設定する。 データにアクセスした利用者を特定できるようなアクセスログを取得できるように設定する。 データベースの操作ログを取得できるように設定する。 VPN回線を利用してクラウドを利用する場合、主体認証ログを取得できるように設定し管理する。	Yes
				データ管理	M	3	ログの使用（閲覧等）可能期間	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の使用（閲覧等）の可能期間が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、可能期間を記述回答欄に記入してください。また、大学・研究機関からの要請により、可能期間を延長または短縮することが可能な場合には、記入してください。	[利用側の施策] 利用するクラウドのログの使用（閲覧等）の可能期間を確認し、大学等で定めたログの保存期間中はログを管理できるようにする。サービスにおけるログの使用可能期間が大学等で定めた保存期間より短い場合には、ログをログサーバ等に保管し、定めたログの保存期間中はログを閲覧できるようにする。	Yes/No
	第四節 情報システムの更改・廃棄	94	D2101-94 （情報システムの更改・廃棄時の対策）（政府機関統一基準の対応項番5.2.4(1)）(p.102) 第九十四条 部局技術責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の措置を適切に講ずること。 一 情報システム更改時の情報の移行作業における情報セキュリティ対策 二 情報システム廃棄時の不要な情報の抹消	データの取り扱い	Q	2	データの削除		カスタマによるデータ削除時の当該データやカスタマの契約終了後のカスタマ情報およびカスタマ所有データが、復元不可能な方法で削除されることが保証されるクラウドを利用する（データの削除証明書を発行してくれるクラウド事業者もある）。 [利用側の施策] カスタマがデータの削除を行う場合は、クラウド事業者から提示された当該データを復元不可能とする削除方法に従って削除を実施する。	Yes
				リソースの引継ぎ	R	1	契約終了時のデータの移行支援	ユーザの都合により契約を終了した時、ユーザがデータ移行の支援を受けることは可能か「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください。	データ移行の支援が受けられるクラウドを利用するか、あるいはクラウドからのデータの取出し方法に関して一括ダウンロードコマンド等の機能およびドキュメンテーションが完備しているクラウドを利用する。	Yes/No
				セキュリティポリシ固有	SA	1	保守を目的としたストレージ機器などの物理的廃棄	サーバやストレージ機器の廃棄や故障による交換を行う場合、内蔵HDD/SSDなどのデータの保存媒体をデータの復元が不可能な方法(物理的破壊、消磁、暗号化キーの廃棄など)で処分しているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください（例：NIST-SP-800-88に準拠した方法でデータをすべて削除する、など）。また、処分を第三者に委託する場合は、データの復元が不可能な方法で処理されたことを監査しているかどうか記入してください。削除証明書の発行が可能な場合には記入してください。	クラウド事業者によるサーバやストレージ機器の廃棄時にデータの復元が不可能な方法で処理されることが保証されるクラウドを利用する。	—

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

第十一章 情報システムのセキュリティ機能	第一節 主体認証機能	98	D2101-98（主体認証に係る対策）（政府機関統一基準の対応項番 6.1.1(1)-1,2）(p.108) 第九十八条 部局技術責任者は、利用者が正当であることを検証するための主体認証機能を設けるに当たっては、以下を例とする主体認証方式を決定し、導入すること。この際、認証の強度として2つ以上の方式を組み合わせる主体認証方式（多要素主体認証方式）が求められる場合には、これを用いること。 一 知識（パスワード等、利用者本人のみが知り得る情報）による認証 二 所有（電子証明書を格納する IC カード又はワンタイムパスワード生成器、利用者本人のみが所有する機器等）による認証 三 生体（指紋や静脈等、本人の生体的な特徴）による認証	認証関連	D	3	多要素認証	多要素認証に対応しているか「Yes/No」欄を選択してください。 「Yes」の場合、本人確認のためにどのような要素を用いているかを記述回答欄に記入してください。	リモートアクセス端末あるいは利用者の認証においては、多要素認証がサポートされているクラウドを利用する。 [利用側の施策] 極力、多要素認証を行う。 ※大学等で運用している多要素認証をサポートしている統合認証ソリューションを利用する場合は、それ経由で利用する個々のクラウドが統合認証サービスと適切に連携できるかどうかを確認するそのクラウド自体が多要素認証をサポートしているかどうかとは別に)。	Yes
	第二節 アクセス制御機能	114	D2101-114（アクセス制御に係る対策)(政府機関統一基準の対応項番 6.1.2(1)-1)(p.116) 第百十四条 部局技術責任者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定めること。また、必要に応じて、以下を例とするアクセス制御機能の要件を定めること。 三 IP アドレスによる端末の制限 四 ネットワークセグメントの分割によるアクセス制御	ネットワーク・通信機能	G	4	アクセス制限機能	サーバを防衛するためのアクセス制限機能がサービスとして提供されているか「Yes/No」欄を選択してください。 「Yes」の場合、アクセス制限の単位（IPアドレス、ポート番号など）を記述回答欄に記入してください。	ネットワークのアクセス制限機能(ファイアウォール、セキュリティグループ、WAF [Web Application Firewall] 等）が提供されているクラウドを利用する。 [利用側の施策] これらの機能の設定を適切に行うことにより通信を制御する。	Yes
				ネットワーク・通信機能	G	6	専用ネットワークセグメント利用の可否	クラウド上にユーザ専用のネットワークセグメントを利用することができるか「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください（事業者からの割り当て、ユーザによる作成など）。	ユーザ専用のネットワークセグメントを利用することが可能なクラウドを利用する。 [利用側の施策] ネットワークセグメントの分割を適切に設計・設定することによりアクセス制御を行う。	Yes
				ネットワーク・通信機能	G	8	IPアドレス制限の可否	ユーザはアクセス元のIPアドレスをもとにアクセス制御を行うことはできるか「Yes/No」欄を選択してください。	アクセス元のIPアドレスに基づいてアクセス制御を行うことの可能なクラウドを利用する。 [利用側の施策] ネットワークセグメントの分割を適切に設計・設定することによりアクセス制御を行う。	Yes
				データ管理	M	7	データのアクセス制限	ユーザが格納したデータごと（例えばファイルごと）にアクセス制限のレベルを任意に設定することができるか 「Yes/No」欄を選択してください。 「Yes」の場合、アクセス制限はどのように行っているか記述回答欄に記入してください（GUIで操作、スクリプトで記述など）。	ファイルやオブジェクトなどのデータの取扱い単位ごとにID・アクセス管理機能を持つクラウドを利用する。 [利用側の施策] データに対するアクセス権限を極力細分化した上で、当機能によって、必要最小限の利用者だけにアクセス権限を与えるよう管理・制御する。	Yes
	第四節 ログの取得・管理	117	D2101-117（ログの取得・管理)(政府機関統一基準の対応項番 6.1.4(1))(p.119) 第百十七条 部局技術責任者は、情報システムにおいて、情報システムが正しく利用されている ことの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得すること。	データ管理	M	1	ログの知的財産権	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の知的財産権がクラウド事業者とユーザ（または契約大学）のいずれに帰属するか、契約書や約款等に明記されているか「Yes/No」欄を選択してください。 「Yes」の場合、契約大学・研究機関が文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	必要なログを取得するために、ログの知的財産権が利用者に帰属するクラウドを利用する。	Yes
				データ管理	M	2	ログの使用権（閲覧等）	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の使用権（閲覧等）がユーザ（または契約大学・研究機関）に認められているか「Yes/No」欄を選択してください。 「Yes」の場合、閲覧できるログの種類を記述回答欄に記入してください。さらに閲覧するログをユーザがダウンロードして保管することが可能であれば記入してください。	必要なログを取得するために、利用するクラウドのログの使用権（閲覧等）が認められているクラウドを利用する。 [追加策/要件に応じて検討] 利用するクラウドの時刻設定が可能な場合には、タイムサーバなどを利用して基準となる時刻に同期させる。また、ログに時刻情報も記録されるように設定する。 データにアクセスした利用者を特定できるようなアクセスログを取得できるように設定する。 データベースの操作ログを取得できるように設定する。 VPN回線を利用してクラウドを利用する場合、主体認証ログを取得できるように設定し管理する。	Yes
				データ管理	M	3	ログの使用（閲覧等）可能期間	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の使用（閲覧等）の可能期間が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、可能期間を記述回答欄に記入してください。また、大学・研究機関からの要請により、可能期間を延長または短縮することが可能な場合には、記入してください。	[利用側の施策] 利用するクラウドのログの使用（閲覧等）の可能期間を確認し、大学等で定めたログの保存期間中はログを管理できるようにする。サービスにおけるログの使用可能期間が大学等で定めた保存期間より短い場合には、ログをログサーバ等に保管し、定めたログの保存期間中はログを閲覧できるようにする。	Yes/No
		119	D2101-119（ログの管理に係る対策)(政府機関統一基準の対応項番 6.1.4(1)-2,3,4)(p.121) 第百十九条 2 部局技術責任者は、取得したログに対する、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、ログ情報の保全方法を定めること。	データ管理	M	7	データのアクセス制限	ユーザが格納したデータごと（例えばファイルごと）にアクセス制限のレベルを任意に設定することができるか 「Yes/No」欄を選択してください。 「Yes」の場合、アクセス制限はどのように行っているか記述回答欄に記入してください（GUIで操作、スクリプトで記述など）。	ファイルやオブジェクトなどのデータの取扱い単位ごとにID・アクセス管理機能を持つクラウドを利用する。 [利用側の施策] データに対するアクセス権限を極力細分化した上で、当機能によって、必要最小限の利用者だけにアクセス権限を与えるよう管理・制御する。	Yes

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

	第五節 暗号・電子署名	125	D2101-125 (暗号化機能・電子署名機能の導入)(政府機関統一基準の対応項番6.1.5(1))(p.126) 第百二十五条 部局技術責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の措置を講ずること。 一 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。 2 部局技術責任者は、暗号技術検討会及び関連委員会(CRYPTREC)により安全性及び実装性 能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、 以下の事項を含めて定めること。 一 利用者等が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。 二 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。	データ管理	M	4	データの暗号化	保存するユーザのデータは暗号化が可能か「Yes/No」欄を選択してください。 「Yes」の場合、暗号化する方式を記述回答欄に記入してください（ユーザが暗号化の要否を選択する、システムが自動で暗号化するなど）。	トランザクションデータおよび保存データの両方に関して「電子政府推奨暗号リスト」に記載された複数の暗号化アルゴリズムおよびそれに基づいた安全なプロトコルを選択することが可能なクラウドを利用する。	Yes
				データ管理	M	5	暗号化鍵の管理方法	ユーザのデータ管理において暗号化に用いる鍵の管理方法は公開されているか「Yes/No」欄を選択してください。 「Yes」の場合、ユーザが確認する方法を記述回答欄に記入してください。	トランザクションデータおよび保存データの両方に関して暗号化が可能なクラウドを利用する場合、暗号化に用いる鍵の管理方法について確認する。 [追加策] カスタマによる鍵管理が可能な場合は、必要に応じて、鍵管理を自前で行うことを検討する。	Yes
		126	D2101-126 (暗号化・電子署名に係る対策)(政府機関統一基準の対応項番6.1.5(1)-1)(p.128) 第百二十六条 部局技術責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずること。 二 複数のアルゴリズム及びそれに基づいた安全なプロトコルを選択することが可能な構成とする。	データ管理	M	4	データの暗号化	保存するユーザのデータは暗号化が可能か「Yes/No」欄を選択してください。 「Yes」の場合、暗号化する方式を記述回答欄に記入してください（ユーザが暗号化の要否を選択する、システムが自動で暗号化するなど）。	トランザクションデータおよび保存データの両方に関して「電子政府推奨暗号リスト」に記載された複数の暗号化アルゴリズムおよびそれに基づいた安全なプロトコルを選択することが可能なクラウドを利用する。	Yes
				データ管理	M	5	暗号化鍵の管理方法	ユーザのデータ管理において暗号化に用いる鍵の管理方法は公開されているか「Yes/No」欄を選択してください。 「Yes」の場合、ユーザが確認する方法を記述回答欄に記入してください。	トランザクションデータおよび保存データの両方に関して暗号化が可能なクラウドを利用する場合、暗号化に用いる鍵の管理方法について確認する。 [追加策] カスタマによる鍵管理が可能な場合は、必要に応じて、鍵管理を自前で行うことを検討する。	Yes
第十二章 情報システムの脅威への対策	第一節 ソフトウェアに関する脆弱性対策	129	D2101-129 (ソフトウェアに関する脆弱性対策の実施)(政府機関統一基準の対応項番6.2.1(1))(p.132) 第百二十九条 部局技術責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、 当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施すること。 3 部局技術責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を定期的に確認すること。 [D2101 p.131] 4 部局技術責任者は、脆弱性対策の状況の定期的な確認により、脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバ ージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。	セキュリティ(全般)	L	5	バージョンアップの頻度	クラウド事業者がサービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、その頻度あるいは基準を記述回答欄に記入してください。	サービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes
				セキュリティ(全般)	L	6	アップデート情報（脆弱性情報）の提供	サーバのメニュー、テンプレート、イメージとして提供されているOS・アプリケーション等のアップデート情報や脆弱性情報はユーザに提供されるか「Yes/No」欄を選択してください。	サービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準がカスタマに文書として開示されているクラウドを利用する。 [追加策] 利用しているサーバに対して可能な範囲で脆弱性診断を実施することを検討する。	Yes
				セキュリティ(全般)	L	7	セキュリティアップデートの自動適用	サーバのメニュー、テンプレート、イメージとして提供されているOS・アプリケーション等の自動セキュリティアップデート機能はユーザに提供されるか「Yes/No」欄を選択してください。	サーバのメニュー、テンプレート、イメージとして提供されているOS・アプリケーション等の自動セキュリティアップデート機能が利用者に提供されているクラウドを利用する。 [追加策] 利用しているサーバに対して可能な範囲で脆弱性診断を実施することを検討する。	Yes
		130	D2101-130 (ソフトウェアに関する脆弱性対策)(政府機関統一基準の対応項番6.2.1(1)-1,2,3,4, 5,6,7,8)(p.133) 第百三十条 部局技術責任者は、対象となるソフトウェアの脆弱性に関して、以下を含む情報を適宜入手すること。 一 脆弱性の原因 二 影響範囲 三 対策方法 四 脆弱性を悪用する不正プログラムの流通状況 3 部局技術責任者は、以下を例とする手段で脆弱性対策の状況を確認すること。 二 脆弱性診断を実施する。 [D2101 p.132] 6 部局技術責任者は、脆弱性対策が計画どおり実施されていることについて、実施予定時期の経過後、遅滞なく確認すること。	セキュリティ(全般)	L	5	バージョンアップの頻度	クラウド事業者がサービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、その頻度あるいは基準を記述回答欄に記入してください。	サービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準が、可能な範囲でカスタマに文書として開示されているクラウドを利用する。	Yes
				セキュリティ(全般)	L	6	アップデート情報（脆弱性情報）の提供	サーバのメニュー、テンプレート、イメージとして提供されているOS・アプリケーション等のアップデート情報や脆弱性情報はユーザに提供されるか「Yes/No」欄を選択してください。	サービスを提供するために用いるサーバのOS・アプリケーションのバージョンアップの頻度あるいは基準がカスタマに文書として開示されているクラウドを利用する。 [追加策] 利用しているサーバに対して可能な範囲で脆弱性診断を実施することを検討する。	Yes
				セキュリティ(全般)	L	7	セキュリティアップデートの自動適用	サーバのメニュー、テンプレート、イメージとして提供されているOS・アプリケーション等の自動セキュリティアップデート機能はユーザに提供されるか「Yes/No」欄を選択してください。	サーバのメニュー、テンプレート、イメージとして提供されているOS・アプリケーション等の自動セキュリティアップデート機能が利用者に提供されているクラウドを利用する。 [追加策] 利用しているサーバに対して可能な範囲で脆弱性診断を実施することを検討する。	Yes

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

第二節 不正プログラム対策	131	D2101-131 （不正プログラム対策の実施)(政府機関統一基準の対応項番 6.2.2(1))(p.136) 第百三十一条 部局技術責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入すること。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。 2 部局技術責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずること。 3 部局技術責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行うこと。	セキュリティ(全般)	L	8	セキュリティ対策	ウイルス検知・防御のサービスが提供されているか「Yes/No」欄を選択してください（IaaS等でユーザが独自にソフトウェアを導入する場合を除く）。「Yes」の場合、基本サービスかオプションサービスかを記述回答欄に記入してください。	不正プログラム対策ソフトウェア(マルウェア検知・防御のサービスなど)が提供されているクラウドを利用し、当該サービスを使用する。 不正プログラム対策ソフトウェアが提供されていないクラウドの場合には、カスタマ側で不正プログラム対策ソフトウェアを導入するなどの対策を行った上で利用する。	Yes/No
	132	D2101-132 （不正プログラム対策ソフトウェア等に係る対策)(政府機関統一基準の対応項番 6.2.2(1)-1,2,3) 第百三十二条 部局技術責任者は、不正プログラム対策ソフトウェア等及びその定義ファイルは、常に最新のものが利用可能となるよう構成すること。 [D2101 p.137]	セキュリティ(全般)	L	9	ウイルス定義の更新	ウイルス検知・防御のサービスが提供されている場合、ウイルス定義ファイルの更新頻度をユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、ユーザが更新頻度を確認する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	不正プログラム対策ソフトウェア(マルウェア検知・防御のサービスなど)のウイルス定義ファイルの更新頻度を確認し、クラウドの不正プログラム対策ソフトウェア(ウイルス検知・防御のサービスなど)等及びその定義ファイルは、常に最新のものが利用可能となるように対策する。	Yes
	134	D2101-134 （不正プログラム対策の状況の把握)(政府機関統一基準の対応項番 6.2.2(1)-5)(p.138) 第百三十四条 部局技術責任者は、不正プログラム対策の実施を徹底するため、以下を例とする不正プログラム対策に関する状況を把握し、必要な対処を行うこと。 一 不正プログラム対策ソフトウェア等の導入状況 二 不正プログラム対策ソフトウェア等の定義ファイルの更新状況	セキュリティ(全般)	L	8	セキュリティ対策	ウイルス検知・防御のサービスが提供されているか「Yes/No」欄を選択してください（IaaS等でユーザが独自にソフトウェアを導入する場合を除く）。「Yes」の場合、基本サービスかオプションサービスかを記述回答欄に記入してください。	不正プログラム対策ソフトウェア(マルウェア検知・防御のサービスなど)が提供されているクラウドを利用し、当該サービスを使用する。 不正プログラム対策ソフトウェアが提供されていないクラウドの場合には、カスタマ側で不正プログラム対策ソフトウェアを導入するなどの対策を行った上で利用する。	Yes/No
			セキュリティ(全般)	L	9	ウイルス定義の更新	ウイルス検知・防御のサービスが提供されている場合、ウイルス定義ファイルの更新頻度をユーザに提示しているか「Yes/No」欄を選択してください。 「Yes」の場合、ユーザが更新頻度を確認する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	不正プログラム対策ソフトウェア(マルウェア検知・防御のサービスなど)のウイルス定義ファイルの更新頻度を確認し、クラウドの不正プログラム対策ソフトウェア(ウイルス検知・防御のサービスなど)等及びその定義ファイルは、常に最新のものが利用可能となるように対策する。	Yes
第四節 標的型攻撃対策	140	D2101-140 （標的型攻撃に係る入口対策)(政府機関統一基準の対応項番 6.2.4(1)-1,2)(p.142) 第百四十条 部局技術責任者は、サーバ装置及び端末について、組織内部への侵入を低減するため、以下を例とする対策を行うこと。 三 パーソナルファイアウォール等を用いて、サーバ装置及び端末に入力される通信及び出力される通信を必要最小限に制限する。	ネットワーク・通信機能	G	4	アクセス制限機能	サーバを防衛するためのアクセス制限機能がサービスとして提供されているか「Yes/No」欄を選択してください。 「Yes」の場合、アクセス制限の単位（IPアドレス、ポート番号など）を記述回答欄に記入してください。	ネットワークのアクセス制限機能(ファイアウォール、セキュリティグループ、WAF [Web Application Firewall] 等) が提供されているクラウドを利用する。 [利用側の施策] これらの機能の設定を適切に行うことにより通信を制御する。	Yes
	141	D2101-141 （標的型攻撃に係る内部対策)(政府機関統一基準の対応項番 6.2.4(1)-3,4,5)(p.144) 第百四十一条 部局技術責任者は、情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定され る、認証サーバやファイルサーバ等の重要サーバについて、以下を例とする対策を行うこと。 一 重要サーバについては、組織内ネットワークを複数セグメントに区切った上で、重要サーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定する。 また、インターネットに直接接続しない。	ネットワーク・通信機能	G	1	SINET接続状況	SINETクラウド接続サービスを提供しているか「Yes/No」欄を選択してください。	[要件に応じて検討] 必要に応じて、SINETクラウド接続サービスを提供しているクラウドを利用し、L2VPNで接続する。	Yes/No
			ネットワーク・通信機能	G	6	専用ネットワークセグメント利用の可否	クラウド上にユーザ専用のネットワークセグメントを利用することができるか「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください（事業者からの割り当て、ユーザによる作成など）。	ユーザ専用のネットワークセグメントを利用することが可能なクラウドを利用する。 [利用側の施策] ネットワークセグメントの分割を適切に設計・設定することによりアクセス制御を行う。	Yes
			ネットワーク・通信機能	G	8	IPアドレス制限の可否	ユーザはアクセス元のIPアドレスをもとにアクセス制御を行うことはできるか「Yes/No」欄を選択してください。	アクセス元のIPアドレスに基づいてアクセス制御を行うことの可能なクラウドを利用する。 [利用側の施策] ネットワークセグメントの分割を適切に設計・設定することによりアクセス制御を行う。	Yes
第十四章 端末・サーバ装置等	第一節 端末	156	D2101-156 （要機密情報を取り扱う本学が支給する端末(要管理対策区域外で使用する場合に 限る)及び本学支給以外の端末の導入及び利用時の対策)(政府機関統一基準の対応項番 7.1.1(4)-1,2)(p.164) 第百五十六条 全学実施責任者は、要機密情報を取り扱う本学が支給する端末(要管理対策区域外で使用する場合に限る)及び本学支給以外の端末について、以下を例に、利用者が端末に情報を保存できないようにするための機能又は端末に保存される情報を暗号化するための機能を設けること。 ニ セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。	データ管理	M	9	データのローカルコピー保持と同期	クラウド上に格納されたデータに対してクライアント側にローカルコピーをもつことは可能か「Yes/No」欄を選択してください。 「Yes」の場合、クラウド上のデータとの同期のタイミングや同期処理の性能について記述回答欄に記入してください。	クライアント側にローカルコピーを作成しない、あるいは作成することを抑止できるクラウドを利用する。 [利用側の施策] 後者の場合は、抑止機能を使用する。	Yes/No
	第二節 サーバ装置	157	D2101-157 （サーバ装置の導入時の対策)(政府機関統一基準の対応項番 7.1.2(1))(p.171) 第百五十七条 部局技術責任者は、要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。 2 部局技術責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについて、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保すること。	管理機能	H	6	フェイルオーバー機能の提供	サーバ間でのフェイルオーバー機能は提供されるか「Yes/No」欄を選択してください。 「Yes」の場合、災害対応など冗長性を考慮しているか記述回答欄に記入してください。	[要件に応じて検討] フェイルオーバー機能が提供されているクラウドの利用を検討する。 ※サーバが停止した場合に自動的に（正常なハードウェア上で）再起動される仕様となっているクラウドもあるので、RTOが厳しくない場合は、その機能を利用することも検討する。	Yes/No
			データセンター	K	1	防犯設備	データセンターにはどのような防犯設備（監視カメラ、警備員常駐、侵入検知センサー、など）を備えているか記述回答欄に記入してください。	防犯設備の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。	記述回答に具体的な記述があるか、適切な情報源が示されている。

				データセンター	K	2	入退室管理体制	データセンターへの入退室をどのように管理（ICカード認証、生体認証、警備員による本人確認、など）しているか記述回答欄に記入してください。健康チェック（検温など）を行っている場合には記入してください。	入退室管理体制の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。	記述回答に具体的な記述があるか、適切な情報源が示されている。
				データセンター	K	4	電力障害対策	データセンターに電力が安定して供給されるよう、監視、二系統受電、自家発電などの対策を行っている場合は記述回答欄に記入してください。災害対応など冗長性を考慮しているか記入してください。	電力障害対策の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。	記述回答に具体的な記述があるか、適切な情報源が示されている。
				データセンター	K	5	ネットワーク障害対策	データセンターのネットワークが安定して運用されるよう、監視や二重化などの対策を行っているか記述回答欄に記入してください。災害対応など冗長性を考慮しているか記入してください。	ネットワーク障害対策の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。 ※本項目は、クラウド基盤の冗長化に関するものであり、高可用性実現のためのシステムとしての冗長化は別途検討が必要である。	記述回答に具体的な記述があるか、適切な情報源が示されている。
				データ管理	M	6	データの多重化	ユーザが格納したデータは多重化されているか 「Yes/No」欄を選択してください。 「Yes」の場合、どのような手法か（RAID、複数データセンターに保存など）記述回答欄に記入してください。災害対応など冗長性を考慮しているか記入してください。	格納データがデータセンタ内で多重化されているサービスを利用する。 [追加策] 必要に応じて、データセンタ間で多重化されている（あるいは多重化可能な）クラウドを利用する。	Yes
		158	D2101-158（物理的な脅威から保護するための対策)(政府機関統一基準の対応項番 7.1.2(1)-1,2,3)(p.172) 第百五十八条 部局技術責任者は、要保護情報を取り扱うサーバ装置については、クラス2以上の要管理対策区域に設置すること。 2 部局技術責任者は、サーバ装置の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。 一 施錠可能なサーバラックに設置して施錠する。 二 容易に切断できないセキュリティワイヤを用いて、固定物又は搬出が困難な物体に固定する。	データセンター	K	1	防犯設備	データセンターにはどのような防犯設備（監視カメラ、警備員常駐、侵入検知センサー、など）を備えているか記述回答欄に記入してください。	防犯設備の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。	記述回答に具体的な記述があるか、適切な情報源が示されている。
				データセンター	K	2	入退室管理体制	データセンターへの入退室をどのように管理（ICカード認証、生体認証、警備員による本人確認、など）しているか記述回答欄に記入してください。健康チェック（検温など）を行っている場合には記入してください。	入退室管理体制の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。	記述回答に具体的な記述があるか、適切な情報源が示されている。
		159	D2101-159（可用性を確保するための対策)(政府機関統一基準の対応項番 7.1.2(1)-4)(p.172) 第百五十九条 部局技術責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため要安定情報を取り扱う情報システムについては、将来の見通しも考慮し、以下を例とする対策を講ずること。 一 負荷分散装置、DNSラウンドロビン方式等による負荷分散 二 同一システムを2系統で構成することによる冗長化	管理機能	H	5	ロードバランサ利用可否	サーバ間でのロードバランサ機能は提供されるか 「Yes/No」欄を選択してください。	[要件に応じて検討] 必要に応じて、ロードバランサ機能が提供されているクラウドの利用を検討する。	Yes/No
				管理機能	H	6	フェイルオーバー機能の提供	サーバ間でのフェイルオーバー機能は提供されるか 「Yes/No」欄を選択してください。 「Yes」の場合、災害対応など冗長性を考慮しているか記述回答欄に記入してください。	[要件に応じて検討] フェイルオーバー機能が提供されているクラウドの利用を検討する。 ※サーバが停止した場合に自動的に（正常なハードウェア上で）再起動される仕様となっているクラウドもあるので、RTOが厳しくない場合は、その機能を利用することも検討する。	Yes/No
				データセンター	K	4	電力障害対策	データセンターに電力が安定して供給されるよう、監視、二系統受電、自家発電などの対策を行っている場合は記述回答欄に記入してください。災害対応など冗長性を考慮しているか記入してください。	電力障害対策の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。	記述回答に具体的な記述があるか、適切な情報源が示されている。
				データセンター	K	5	ネットワーク障害対策	データセンターのネットワークが安定して運用されるよう、監視や二重化などの対策を行っているか記述回答欄に記入してください。災害対応など冗長性を考慮しているか記入してください。	ネットワーク障害対策の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する（たとえばJDCC tier3（相当））。 ※本項目は、クラウド基盤の冗長化に関するものであり、高可用性実現のためのシステムとしての冗長化は別途検討が必要である。	記述回答に具体的な記述があるか、適切な情報源が示されている。
		161	D2101-161（サーバ装置の運用時の対策)(政府機関統一基準の対応項番 7.1.2(2))(p.173) 第百六十一条 3 部局技術責任者は、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を検知する必要がある場合は、当該サーバ装置を監視するための措置を講ずること。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りではない。 4 部局技術責任者は、要安定情報を取り扱うサーバ装置について、サーバ装置が運用できなくなった場合に正常な運用状態に復元することが可能になるよう、必要な措置を講ずること。	セキュリティ(全般)	L	10	ログ分析・脅威検出	ログ分析やセキュリティ上の脅威の自動検出を行う機能（SIEM(Security Information and Event Management)、CASB(Cloud Access Security Broker)等）が提供されるか「Yes/No」欄を選択してください。 「Yes」の場合、具体的な機能を記述回答欄に記入してください。	[要件に応じて検討] 内部および外部からの不正アクセスのチェック・分析の頻度や分析の精度を高める必要がある場合、専任の分析担当者の設置、ログ分析やセキュリティ上の脅威の自動検出を行う機能の利用、監視事業者への委託(F4, F5)を検討する 。	Yes/No
				セキュリティ(全般)	L	11	IDS・IPS	IDS（不正侵入検知システム）・IPS（不正侵入予防システム）はサービスとして提供されているか「Yes/No」欄を選択してください。	[要件に応じて検討] 必要に応じて、IDS（不正侵入検知システム）/IPS（不正侵入予防システム）が提供されているクラウドを利用し、当該機能を使用する。 IPS/IDSが提供されていないクラウドの場合には、カスタマ側でこれらのシステムを導入するなどの対策を行った上で利用する。	Yes/No

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

				データ管理	M	2	ログの使用権（閲覧等）	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の使用権（閲覧等）がユーザ（または契約大学・研究機関）に認められているか「Yes/No」欄を選択してください。 「Yes」の場合、閲覧できるログの種類を記述回答欄に記入してください。さらに閲覧するログをユーザがダウンロードして保管することが可能であれば記入してください。	必要なログを取得するために、利用するクラウドのログの使用権（閲覧等）が認められているクラウドを利用する。 [追加策/要件に応じて検討] 利用するクラウドの時刻設定が可能な場合には、タイムサーバなどを利用して基準となる時刻に同期させる。また、ログに時刻情報も記録されるように設定する。 データにアクセスした利用者を特定できるようなアクセスログを取得できるように設定する。 データベースの操作ログを取得できるように設定する。 VPN回線を利用してクラウドを利用する場合、主体認証ログを取得できるように設定し管理する。	Yes
				データ管理	M	3	ログの使用（閲覧等）可能期間	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の使用（閲覧等）の可能期間が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、可能期間を記述回答欄に記入してください。また、大学・研究機関からの要請により、可能期間を延長または短縮することが可能な場合には、記入してください。	[利用側の施策] 利用するクラウドのログの使用（閲覧等）の可能期間を確認し、大学等で定めたログの保存期間中はログを管理できるようにする。サービスにおけるログの使用可能期間が大学等で定めた保存期間より短い場合には、ログをログサーバ等に保管し、定めたログの保存期間中はログを閲覧できるようにする。	Yes/No
				バックアップ	N	1	バックアップサービスの有無	ユーザがクラウドに格納したデータあるいはユーザが作成したサーバイメージのバックアップを行うサービスは提供されているか「Yes/No」欄を選択してください。（管理者権限をもったユーザのスクリプト等による実現は除く）。	バックアップサービスを提供しているクラウドの場合はその機能を利用する。 提供していないクラウドの場合は、利用者側でバックアップを取得する。	Yes/No
				バックアップ	N	5	バックアップからのリストア	バックアップデータのリストアはユーザ自身で作業できるか「Yes/No」欄を選択してください。 「No」の場合、クラウド事業者作業の依頼手順を記述回答欄に記入してください。	バックアップデータのリストアをカスタマ自身で作業できるクラウドであれば、カスタマ自身の作業を前提としたリカバリ計画を策定する。 バックアップデータのリストアをカスタマ側で作業できないクラウドの場合、リストア作業を行う主体やその仕様（作業手順、タイミング等）について確認した上で利用する。	Yes/No
		163	D2101-163（サーバ装置の監視に係る対策)(政府機関統一基準の対応項番 7.1.2(2)-2)(p.174) 第百六十三条 部局技術責任者は、サーバ装置への無許可のアクセス等の不正な行為を監視するために、以下を例とする対策を講ずること。 一 アクセスログ等を定期的に確認する。 二 IDS/IPS、WAF 等を設置する。	ネットワーク・通信機能	G	4	アクセス制限機能	サーバを防衛するためのアクセス制限機能がサービスとして提供されているか「Yes/No」欄を選択してください。 「Yes」の場合、アクセス制限の単位（IPアドレス、ポート番号など）を記述回答欄に記入してください。	ネットワークのアクセス制限機能(ファイアウォール、セキュリティグループ、WAF [Web Application Firewall] 等）が提供されているクラウドを利用する。 [利用側の施策] これらの機能の設定を適切に行うことにより通信を制御する。	Yes
				セキュリティ(全般)	L	10	ログ分析・脅威検出	ログ分析やセキュリティ上の脅威の自動検出を行う機能（SIEM(Security Information and Event Management)、CASB(Cloud Access Security Broker)等）が提供されるか「Yes/No」欄を選択してください。 「Yes」の場合、具体的な機能を記述回答欄に記入してください。	[要件に応じて検討] 内部および外部からの不正アクセスのチェック・分析の頻度や分析の精度を高める必要がある場合、専任の分析担当者の設置、ログ分析やセキュリティ上の脅威の自動検出を行う機能の利用、監視事業者への委託(F4, F5)を検討する 。	Yes/No
				セキュリティ(全般)	L	11	IDS・IPS	IDS（不正侵入検知システム）・IPS（不正侵入予防システム）はサービスとして提供されているか「Yes/No」欄を選択してください。	[要件に応じて検討] 必要に応じて、IDS（不正侵入検知システム）/IPS（不正侵入予防システム）が提供されているクラウドを利用し、当該機能を使用する。 IPS/IDSが提供されていないクラウドの場合には、カスタマ側でこれらのシステムを導入するなどの対策を行った上で利用する。	Yes/No
				データ管理	M	1	ログの知的財産権	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の知的財産権がクラウド事業者とユーザ（または契約大学）のいずれに帰属するか、契約書や約款等に明記されているか「Yes/No」欄を選択してください。 「Yes」の場合、契約大学・研究機関が文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	必要なログを取得するために、ログの知的財産権が利用者に帰属するクラウドを利用する。	Yes
				データ管理	M	2	ログの使用権（閲覧等）	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の使用権（閲覧等）がユーザ（または契約大学・研究機関）に認められているか「Yes/No」欄を選択してください。 「Yes」の場合、閲覧できるログの種類を記述回答欄に記入してください。さらに閲覧するログをユーザがダウンロードして保管することが可能であれば記入してください。	必要なログを取得するために、利用するクラウドのログの使用権（閲覧等）が認められているクラウドを利用する。 [追加策/要件に応じて検討] 利用するクラウドの時刻設定が可能な場合には、タイムサーバなどを利用して基準となる時刻に同期させる。また、ログに時刻情報も記録されるように設定する。 データにアクセスした利用者を特定できるようなアクセスログを取得できるように設定する。 データベースの操作ログを取得できるように設定する。 VPN回線を利用してクラウドを利用する場合、主体認証ログを取得できるように設定し管理する。	Yes

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

				データ管理	M	3	ログの使用（閲覧等）可能期間	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の使用（閲覧等）の可能期間が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、可能期間を記述回答欄に記入してください。また、大学・研究機関からの要請により、可能期間を延長または短縮することが可能な場合には、記入してください。	[利用側の施策] 利用するクラウドのログの使用（閲覧等）の可能期間を確認し、大学等で定めたログの保存期間中はログを管理できるようにする。サービスにおけるログの使用可能期間が大学等で定めた保存期間より短い場合には、ログをログサーバ等に保管し、定めたログの保存期間中はログを閲覧できるようにする。	Yes/No
		164	D2101-164（サーバ装置の復元に係る対策)(政府機関統一基準の対応項番 7.1.2(2)-3)(p.175) 第百六十四条 部局技術責任者は、要安定情報を取り扱うサーバ装置については、運用状態を復元するために以下を例とする対策を講ずること。 二 定期的なバックアップを実施する。	バックアップ	N	1	バックアップサービスの有無	ユーザがクラウドに格納したデータあるいはユーザが作成したサーバイメージのバックアップを行うサービスは提供されているか「Yes/No」欄を選択してください。（管理者権限をもったユーザのスクリプト等による実現は除く）。	バックアップサービスを提供しているクラウドの場合はその機能を利用する。 提供していないクラウドの場合は、利用者側でバックアップを取得する。	Yes/No
				バックアップ	N	3	バックアップの世代管理	複数世代のバックアップを取得・管理することは可能か「Yes/No」欄を選択してください。 「Yes」の場合、世代数の上限やフルバックアップ・差分バックアップの選択は可能か記述回答欄に記入してください。	[要件に応じて検討] クラウドが提供するバックアップサービスを利用する際に、複数世代のバックアップ取得・管理が必要な場合には本機能を利用する。	Yes/No
				バックアップ	N	4	複数センターへの同時バックアップ可否	バックアップ先として同一インフラストラクチャ、別インフラストラクチャ、別データセンタ、別地域などを指定することは可能か「Yes/No」欄を選択してください。 「Yes」の場合、これらの複数のバックアップ先のバックアップデータの一貫性を維持することは可能か記述回答欄に記入してください。また、特に災害対応を考慮する場合、バックアップ先をどのように指定すればよいか記入してください。	[要件に応じて検討] クラウドが提供するバックアップサービスを利用する際に、複数のセンターへの同時バックアップが必要な場合は本機能を利用する。	Yes/No
				バックアップ	N	5	バックアップからのリストア	バックアップデータのリストアはユーザ自身で作業できるか「Yes/No」欄を選択してください。 「No」の場合、クラウド事業者作業の依頼手順を記述回答欄に記入してください。	バックアップデータのリストアをカスタマ自身で作業できるクラウドであれば、カスタマ自身の作業を前提としたリカバリ計画を策定する。 バックアップデータのリストアをカスタマ側で作業できないクラウドの場合、リストア作業を行う主体やその仕様（作業手順、タイミング等）について確認した上で利用する。	Yes/No
		165	D2101-165（サーバ装置の運用終了時の対策)(政府機関統一基準の対応項番 7.1.2(3))(p.175) 第百六十五条 部局技術責任者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消すること。	データの取り扱い	Q	2	データの削除	ユーザがデータを明に削除した時の当該データ、あるいはユーザの都合により契約を終了した後のユーザ情報およびユーザが所有していた全データが再利用されないことが保証されているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください（例：NIST-SP-800-88に準拠した方法でデータをすべて削除する、など）。削除証明書の発行が可能な場合には記入してください。	カスタマによるデータ削除時の当該データやカスタマの契約終了後のカスタマ情報およびカスタマ所有データが、復元不可能な方法で削除されることが保証されるクラウドを利用する（データの削除証明書を発行してくれるクラウド事業者もある）。 [利用側の施策] カスタマがデータの削除を行う場合は、クラウド事業者から提示された当該データを復元不可能とする削除方法に従って削除を実施する。	Yes
				セキュリティポリシ固有	SA	1	保守を目的としたストレージ機器などの物理的廃棄	サーバやストレージ機器の廃棄や故障による交換を行う場合、内蔵HDD/SSDなどのデータの保存媒体をデータの復元が不可能な方法(物理的破壊、消磁、暗号化キーの廃棄など)で処分しているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください（例：NIST-SP-800-88に準拠した方法でデータをすべて削除する、など）。また、処分を第三者に委託する場合は、データの復元が不可能な方法で処理されたことを監査しているかどうか記入してください。削除証明書の発行が可能な場合には記入してください。	クラウド事業者によるサーバやストレージ機器の廃棄時にデータの復元が不可能な方法で処理されることが保証されるクラウドを利用する。	—
	第四節 データベース	186	D2101-186（データベースの導入・運用時の対策)(政府機関統一基準の対応項番 7.2.4(1))(p.201) 第百八十六条 部局技術責任者は、データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行うこと。 2 部局技術責任者は、データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずること。 3 部局技術責任者は、データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずること。 5 部局技術責任者は、データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化をすること。	管理機能	H	1	管理者権限	ユーザは利用するサーバの管理者権限（Linux等：root権限、Windows：Administrator権限）を与えられるか「Yes/No」欄を選択してください。	管理者権限の与えられているクラウドを利用する。 [利用側の施策] 管理者アカウントの権限管理を適正に行う。	Yes
				管理機能	H	10	IDとアクセス管理	ユーザ、およびユーザ権限の管理機能は提供されるか「Yes/No」欄を選択してください。	IDとアクセス管理機能（IDおよびそのIDの権限の管理機能）が提供されているクラウドを利用する。 [利用側の施策] 当機能によって、クラウドに格納された要機密情報のアクセス管理(ダウンロード等の操作も想定して)や、管理者アカウントの適正な権限管理を行う。	Yes

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

				セキュリティ(全般)	L	10	ログ分析・脅威検出	ログ分析やセキュリティ上の脅威の自動検出を行う機能（SIEM(Security Information and Event Management)、CASB(Cloud Access Security Broker)等）が提供されるか「Yes/No」欄を選択してください。 「Yes」の場合、具体的な機能を記述回答欄に記入してください。	[要件に応じて検討] 内部および外部からの不正アクセスのチェック・分析の頻度や分析の精度を高める必要がある場合、専任の分析担当者の設置、ログ分析やセキュリティ上の脅威の自動検出を行う機能の利用、監視事業者への委託(F4, F5)を検討する 。	Yes/No
				セキュリティ(全般)	L	11	IDS・IPS	IDS（不正侵入検知システム）・IPS（不正侵入予防システム）はサービスとして提供されているか「Yes/No」欄を選択してください。	[要件に応じて検討] 必要に応じて、IDS（不正侵入検知システム）/IPS（不正侵入予防システム）が提供されているクラウドを利用し、当該機能を使用する。 IPS/IDSが提供されていないクラウドの場合には、カスタマ側でこれらのシステムを導入するなどの対策を行った上で利用する。	Yes/No
				データ管理	M	1	ログの知的財産権	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の知的財産権がクラウド事業者とユーザ（または契約大学）のいずれに帰属するか、契約書や約款等に明記されているか「Yes/No」欄を選択してください。 「Yes」の場合、契約大学・研究機関が文書を閲覧する方法（ウェブページに掲載、契約時に書面交付など）を記述回答欄に記入してください。	必要なログを取得するために、ログの知的財産権が利用者に帰属するクラウドを利用する。	Yes
				データ管理	M	2	ログの使用権（閲覧等）	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の使用権（閲覧等）がユーザ（または契約大学・研究機関）に認められているか「Yes/No」欄を選択してください。 「Yes」の場合、閲覧できるログの種類を記述回答欄に記入してください。さらに閲覧するログをユーザがダウンロードして保管することが可能であれば記入してください。	必要なログを取得するために、利用するクラウドのログの使用権（閲覧等）が認められているクラウドを利用する。 [追加策/要件に応じて検討] 利用するクラウドの時刻設定が可能な場合には、タイムサーバなどを利用して基準となる時刻に同期させる。また、ログに時刻情報も記録されるように設定する。 データにアクセスした利用者を特定できるようなアクセスログを取得できるように設定する。 データベースの操作ログを取得できるように設定する。 VPN回線を利用してクラウドを利用する場合、主体認証ログを取得できるように設定し管理する。	Yes
				データ管理	M	3	ログの使用（閲覧等）可能期間	アプリケーションログ（SaaS、IDaaS）あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ（IaaS）の使用（閲覧等）の可能期間が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、可能期間を記述回答欄に記入してください。また、大学・研究機関からの要請により、可能期間を延長または短縮することが可能な場合には、記入してください。	[利用側の施策] 利用するクラウドのログの使用（閲覧等）の可能期間を確認し、大学等で定めたログの保存期間中はログを管理できるようにする。サービスにおけるログの使用可能期間が大学等で定めた保存期間より短い場合には、ログをログサーバ等に保管し、定めたログの保存期間中はログを閲覧できるようにする。	Yes/No
				データ管理	M	4	データの暗号化	保存するユーザのデータは暗号化が可能か「Yes/No」欄を選択してください。 「Yes」の場合、暗号化する方式を記述回答欄に記入してください（ユーザが暗号化の要否を選択する、システムが自動で暗号化するなど）。	トランザクションデータおよび保存データの両方に関して「電子政府推奨暗号リスト」に記載された複数の暗号化アルゴリズムおよびそれに基づいた安全なプロトコルを選択することが可能なクラウドを利用する。	Yes
				データ管理	M	5	暗号化鍵の管理方法	ユーザのデータ管理において暗号化に用いる鍵の管理方法は公開されているか「Yes/No」欄を選択してください。 「Yes」の場合、ユーザが確認する方法を記述回答欄に記入してください。	トランザクションデータおよび保存データの両方に関して暗号化が可能なクラウドを利用する場合、暗号化に用いる鍵の管理方法について確認する。 [追加策] カスタマによる鍵管理が可能な場合は、必要に応じて、鍵管理を自前で行うことを検討する。	Yes
		189	D2101-189 （データベースにおける脆弱性に係る対策）(政府機関統一基準の対応項番 7.2.4(1)-5,6)(p.203) 第百八十九条 一 ウェブアプリケーションファイアウォールの導入 二 データベースファイアウォールの導入	ネットワーク・通信機能	G	4	アクセス制限機能	サーバを防衛するためのアクセス制限機能がサービスとして提供されているか「Yes/No」欄を選択してください。 「Yes」の場合、アクセス制限の単位（IPアドレス、ポート番号など）を記述回答欄に記入してください。	ネットワークのアクセス制限機能(ファイアウォール、セキュリティグループ、WAF [Web Application Firewall] 等）が提供されているクラウドを利用する。 [利用側の施策] これらの機能の設定を適切に行うことにより通信を制御する。	Yes
		190	D2101-190 （データベースにおける暗号化に係る対策）(政府機関統一基準の対応項番 7.2.4(1)-7)(p.203) 第百九十条 部局技術責任者は、格納されているデータに対して暗号化を実施する場合には、バックアップデータやトランザクションデータ等についても暗号化を実施すること。	データ管理	M	4	データの暗号化	保存するユーザのデータは暗号化が可能か「Yes/No」欄を選択してください。 「Yes」の場合、暗号化する方式を記述回答欄に記入してください（ユーザが暗号化の要否を選択する、システムが自動で暗号化するなど）。	トランザクションデータおよび保存データの両方に関して「電子政府推奨暗号リスト」に記載された複数の暗号化アルゴリズムおよびそれに基づいた安全なプロトコルを選択することが可能なクラウドを利用する。	Yes
				データ管理	M	5	暗号化鍵の管理方法	ユーザのデータ管理において暗号化に用いる鍵の管理方法は公開されているか「Yes/No」欄を選択してください。 「Yes」の場合、ユーザが確認する方法を記述回答欄に記入してください。	トランザクションデータおよび保存データの両方に関して暗号化が可能なクラウドを利用する場合、暗号化に用いる鍵の管理方法について確認する。 [追加策] カスタマによる鍵管理が可能な場合は、必要に応じて、鍵管理を自前で行うことを検討する。	Yes

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

				バックアップ	N	6	バックアップデータのセキュリティ	バックアップデータのアクセス制限や暗号化に関して、元のデータと同等のセキュリティレベルが継承されているか「Yes/No」欄を選択してください。	バックアップデータに対して元データと同等のセキュリティレベルが実現されるクラウドを利用する。 [利用側の施策] 必要な場合はそれが可能となる設定や利用方法を実施する。	Yes
第十六章 通信回線	第一節 通信回線	191	D2101-191 (通信回線の導入時の対策)(政府機関統一基準の対応項番 7.3.1(1))(p.203) 第百九十一条 3 部局技術責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずること。 4 部局技術責任者は、利用者等が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。 6 部局技術責任者は、要安定情報を取り扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずること。	ネットワーク・通信機能	G	1	SINET接続状況	SINETクラウド接続サービスを提供しているか「Yes/No」欄を選択してください。	[要件に応じて検討] 必要に応じて、SINETクラウド接続サービスを提供しているクラウドを利用し、L2VPNで接続する。	Yes/No
				ネットワーク・通信機能	G	2	通信のセキュリティ確保	端末からサーバまでの通信のセキュリティ確保がサービスとして提供されているか「Yes/No」欄を選択してください。 「Yes」の場合、どのようにセキュリティを確保しているか、方式(SSHやSSL/TLSによる暗号化、ファイル共有におけるAES、SINET L2VPN、IPsec、SSL-VPN等)を記述回答欄に記入してください。	端末からサーバまでの通信に関して、「電子政府推奨暗号リスト」に記載された複数の暗号化アルゴリズムおよびそれに基づいた安全なプロトコルを選択することが可能なクラウドを利用する。 [追加策] VPN回線でクラウドを利用する場合、二重の暗号化を行う(例えば、インターネット VPN 回線において IPsec で通信経路の暗号化を行った上で HTTPS 通信によりコンテンツの暗号化を行 う)などを考慮する。	Yes
				ネットワーク・通信機能	G	8	IPアドレス制限の可否	ユーザはアクセス元のIPアドレスをもとにアクセス制御を行うことはできるか「Yes/No」欄を選択してください。	アクセス元のIPアドレスに基づいてアクセス制御を行うことの可能なクラウドを利用する。 [利用側の施策] ネットワークセグメントの分割を適切に設計・設定することによりアクセス制御を行う。	Yes
				データセンタ	K	5	ネットワーク障害対策	データセンターのネットワークが安定して運用されるよう、監視や二重化などの対策を行っているか記述回答欄に記入してください。災害対応など冗長性を考慮しているか記入してください。	ネットワーク障害対策の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する (たとえばJDCC tier3 (相当))。 ※本項目は、クラウド基盤の冗長化に関するものであり、高可用性実現のためのシステムとしての冗長化は別途検討が必要である。	記述回答に具体的な記述があるか、適切な情報源が示されている。
		192	D2101-192 (通信経路の分離に係る対策)(政府機関統一基準の対応項番 7.3.1(1)-1)(p.205) 第百九十二条 部局技術責任者は、通信回線を経由した情報セキュリティインシデントの影響範 囲を限定的にするため、通信回線の構成、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じて、以下を例とする通信経路の分離を行うこと。 二 業務目的や取り扱う情報の格付及び取扱制限に応じて情報システムごとにVLANにより通信経路を分離し、それぞれの通信制御を適切に行う。	ネットワーク・通信機能	G	6	専用ネットワークセグメント利用の可否	クラウド上にユーザ専用のネットワークセグメントを利用することができるか「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください(事業者からの割り当て、ユーザによる作成など)。	ユーザ専用のネットワークセグメントを利用することが可能なクラウドを利用する。 [利用側の施策] ネットワークセグメントの分割を適切に設計・設定することによりアクセス制御を行う。	Yes
				管理機能	H	4	ネットワーク構成機能	ユーザがネットワークの構成を変更する機能は提供されるか「Yes/No」欄を選択してください。	ネットワーク構成機能が提供されているクラウドを利用する。 [利用側の施策] 当機能によってVLANを構成することで通信経路を分離し、それぞれの通信を制御する。	Yes
		193	D2101-193 (通信回線の秘匿性確保に係る対策)(政府機関統一基準の対応項番 7.3.1(1)-2)(p.205) 第百九十三条 部局技術責任者は、通信経路における盗聴及び情報の改ざん等の脅威への対策として、通信内容の秘匿性を確保するための機能を設けること。通信回線の秘匿性確保の方法として、TLS(SSL)、IPsec 等による暗号化を行うこと。	ネットワーク・通信機能	G	2	通信のセキュリティ確保	端末からサーバまでの通信のセキュリティ確保がサービスとして提供されているか「Yes/No」欄を選択してください。 「Yes」の場合、どのようにセキュリティを確保しているか、方式(SSHやSSL/TLSによる暗号化、ファイル共有におけるAES、SINET L2VPN、IPsec、SSL-VPN等)を記述回答欄に記入してください。	端末からサーバまでの通信に関して、「電子政府推奨暗号リスト」に記載された複数の暗号化アルゴリズムおよびそれに基づいた安全なプロトコルを選択することが可能なクラウドを利用する。 [追加策] VPN回線でクラウドを利用する場合、二重の暗号化を行う(例えば、インターネット VPN 回線において IPsec で通信経路の暗号化を行った上で HTTPS 通信によりコンテンツの暗号化を行 う)などを考慮する。	Yes
		194	D2101-194 (通信回線への情報システムの接続に係る対策)(政府機関統一基準の対応項番 7.3.1(1)-3)(p.206) 第百九十四条 部局技術責任者は、学内通信回線への接続を許可された情報システムであることを確認し、無許可の情報システムの接続を拒否するための機能として、以下を例とする対策を講ずること。 一 情報システムの機器番号等により接続機器を識別する。	ネットワーク・通信機能	G	8	IPアドレス制限の可否	ユーザはアクセス元のIPアドレスをもとにアクセス制御を行うことはできるか「Yes/No」欄を選択してください。	アクセス元のIPアドレスに基づいてアクセス制御を行うことの可能なクラウドを利用する。 [利用側の施策] ネットワークセグメントの分割を適切に設計・設定することによりアクセス制御を行う。	Yes
		196	D2101-196 (要安定情報を取り扱う情報システムが接続される通信回線に係る対策)(政府機関 統一基準の対応項番 7.3.1(1)-5)(p.206) 第百九十六条 部局技術責任者は、要安定情報を取り扱う情報システムが接続される通信回線を構築する場合は、以下を例とする対策を講ずること。 一 通信回線の性能低下や異常の有無を確認するため、通信回線の利用率、接続率等の運用状態を定常的に確認、分析する機能を設ける。 二 通信回線及び通信回線装置を冗長構成にする。	管理機能	H	11	利用統計	サービスへのアクセス数やリソースの利用率など、利用統計を取得する機能は提供されるか「Yes/No」欄を選択してください。 「Yes」の場合、どのような統計が取得可能か記述回答欄に記入してください。	利用統計を取得できるクラウドを利用する。 [利用側の施策] 当機能によって通信回線の通信量、接続率等の運用状態を定常的に確認・記録・分析し、サーバやネットワークの資源を適切に分配・管理する。	Yes
				データセンター	K	5	ネットワーク障害対策	データセンターのネットワークが安定して運用されるよう、監視や二重化などの対策を行っているか記述回答欄に記入してください。災害対応など冗長性を考慮しているか記入してください。	ネットワーク障害対策の整ったデータセンターで運用されていると判断できる情報が提供されているクラウドを利用する。あるいは一定のデータセンターファシリティ基準を満たすクラウドを利用する (たとえばJDCC tier3 (相当))。 ※本項目は、クラウド基盤の冗長化に関するものであり、高可用性実現のためのシステムとしての冗長化は別途検討が必要である。	記述回答に具体的な記述があるか、適切な情報源が示されている。
		197	D2101-197 (学内通信回線と学外通信回線との接続に係る対策)(政府機関統一基準の対応項番 7.3.1(1)-6)(p.207) 第百九十七条 部局技術責任者は、学内通信回線に、インターネット回線や公衆通信回線等の学外通信回線を接続する場合には、外部からの不正アクセスによる被害を防止するため、以下を 例とする対策を講ずること。	ネットワーク・通信機能	G	4	アクセス制限機能	サーバを防衛するためのアクセス制限機能がサービスとして提供されているか「Yes/No」欄を選択してください。 「Yes」の場合、アクセス制限の単位(IPアドレス、ポート番号など)を記述回答欄に記入してください。	ネットワークのアクセス制限機能(ファイアウォール、セキュリティグループ、WAF [Web Application Firewall] 等) が提供されているクラウドを利用する。 [利用側の施策] これらの機能の設定を適切に行うことにより通信を制御する。	Yes

			ー ファイアウォール、WAF(WebApplicationFirewall)等により通信制御を行う。 三 IDS/IPS により不正アクセスを検知及び遮断する。	セキュリティ(全般)	L	10	ログ分析・脅威検出	ログ分析やセキュリティ上の脅威の自動検出を行う機能（SIEM(Security Information and Event Management)、CASB(Cloud Access Security Broker)等）が提供されるか「Yes/No」欄を選択してください。 「Yes」の場合、具体的な機能を記述回答欄に記入してください。	[要件に応じて検討] 内部および外部からの不正アクセスのチェック・分析の頻度や分析の精度を高める必要がある場合、専任の分析担当者の設置、ログ分析やセキュリティ上の脅威の自動検出を行う機能の利用、監視事業者への委託(F4, F5)を検討する 。	Yes/No
				セキュリティ(全般)	L	11	IDS・IPS	IDS（不正侵入検知システム）・IPS（不正侵入予防システム）はサービスとして提供されているか「Yes/No」欄を選択してください。	[要件に応じて検討] 必要に応じて、IDS（不正侵入検知システム）/IPS（不正侵入予防システム）が提供されているクラウドを利用し、当該機能を使用する。 IPS/IDSが提供されていないクラウドの場合には、カスタマ側でこれらのシステムを導入するなどの対策を行った上で利用する。	Yes/No
		201	D2101-201 (通信回線の運用終了時の対策)(政府機関統一基準の対応項番 7.3.1(3))(p.209) 第二百一条 部局技術責任者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど適切な措置を講ずること。	データの取り扱い	Q	2	データの削除	ユーザがデータを明に削除した時の当該データ、あるいはユーザの都合により契約を終了した後のユーザ情報およびユーザが所有していた全データが再利用されないことが保証されているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください（例：NIST-SP-800-88に準拠した方法でデータをすべて削除する、など）。削除証明書の発行が可能な場合には記入してください。	カスタマによるデータ削除時の当該データやカスタマの契約終了後のカスタマ情報およびカスタマ所有データが、復元不可能な方法で削除されることが保証されるクラウドを利用する（データの削除証明書を発行してくれるクラウド事業者もある）。 [利用側の施策] カスタマがデータの削除を行う場合は、クラウド事業者から提示された当該データを復元不可能とする削除方法に従って削除を実施する。	Yes
				セキュリティポリシ固有	SA	1	保守を目的としたストレージ機器などの物理的廃棄	サーバやストレージ機器の廃棄や故障による交換を行う場合、内蔵HDD/SSDなどのデータの保存媒体をデータの復元が不可能な方法(物理的破壊、消磁、暗号化キーの廃棄など)で処分しているか「Yes/No」欄を選択してください。 「Yes」の場合、その方法を記述回答欄に記入してください（例：NIST-SP-800-88に準拠した方法でデータをすべて削除する、など）。また、処分を第三者に委託する場合は、データの復元が不可能な方法で処理されたことを監査しているかどうか記入してください。削除証明書の発行が可能な場合には記入してください。	クラウド事業者によるサーバやストレージ機器の廃棄時にデータの復元が不可能な方法で処理されることが保証されるクラウドを利用する。	—
		202	D2101-202 (リモートアクセス環境導入時の対策)(政府機関統一基準の対応項番 7.3.1(4))(p.209) 第二百二条 部局技術責任者は、VPN回線を整備する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずること。	認証関連	D	2	SAML認証連携（Shibboleth利用可否）	SAMLによるユーザ認証連携は可能か「Yes/No」欄を選択してください。 「Yes」の場合、Shibbolethによるユーザ認証連携の実績があれば記述回答欄に記入してください。 「No」の場合、SAML以外でユーザ認証連携可能なものがあれば記述回答欄に記入してください。	[要件に応じて検討] リモートアクセス端末あるいは利用者の認証において、学認利用のポリシがある場合には、SAML認証連携が可能なクラウドを利用する。	Yes/No
				認証関連	D	3	多要素認証	多要素認証に対応しているか「Yes/No」欄を選択してください。 「Yes」の場合、本人確認のためにどのような要素を用いているかを記述回答欄に記入してください。	リモートアクセス端末あるいは利用者の認証においては、多要素認証がサポートされているクラウドを利用する。 [利用側の施策] 極力、多要素認証を行う。 ※大学等で運用している多要素認証をサポートしている統合認証ソリューションを利用する場合は、それ経由で利用する個々のクラウドが統合認証サービスと適切に連携できるかどうかを確認するそのクラウド自体が多要素認証をサポートしているかどうかとは別に)。	Yes
				ネットワーク・通信機能	G	1	SINET接続状況	SINETクラウド接続サービスを提供しているか「Yes/No」欄を選択してください。	[要件に応じて検討] 必要に応じて、SINETクラウド接続サービスを提供しているクラウドを利用し、L2VPNで接続する。	Yes/No
				ネットワーク・通信機能	G	2	通信のセキュリティ確保	端末からサーバまでの通信のセキュリティ確保がサービスとして提供されているか「Yes/No」欄を選択してください。 「Yes」の場合、どのようにセキュリティを確保しているか、方式（SSHやSSL/TLSによる暗号化、ファイル共有におけるAES、SINET L2VPN、IPsec、SSL-VPN等）を記述回答欄に記入してください。	端末からサーバまでの通信に関して、「電子政府推奨暗号リスト」に記載された複数の暗号化アルゴリズムおよびそれに基づいた安全なプロトコルを選択することが可能なクラウドを利用する。 [追加策] VPN回線でクラウドを利用する場合、二重の暗号化を行う（例えば、インターネット VPN 回線において IPsec で通信経路の暗号化を行った上で HTTPS 通信によりコンテンツの暗号化を行 う)などを考慮する。	Yes

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp

		203	D2101-203 (VPN 回線によるリモートアクセス環境に係る対策)(政府機関統一基準の対応項 番 7.3.1(4)-1)(p.209) 第二百三条 部局技術責任者は、VPN 回線を整備してリモートアクセス環境を構築する場合は、以下を例とする対策を講ずること。 二 通信を行う端末の識別又は認証 三 利用者の認証 四 通信内容の暗号化 五 主体認証ログの取得及び管理	認証関連	D	2	SAML認証連携 (Shibboleth利用可否)	SAMLによるユーザ認証連携は可能か「Yes/No」欄を選択してください。 「Yes」の場合、Shibbolethによるユーザ認証連携の実績があれば記述回答欄に記入してください。 「No」の場合、SAML以外でユーザ認証連携可能なものがあれば記述回答欄に記入してください。	[要件に応じて検討] リモートアクセス端末あるいは利用者の認証において、学認利用のポリシがある場合には、SAML認証連携が可能なクラウドを利用する。	Yes/No
				認証関連	D	3	多要素認証	多要素認証に対応しているか「Yes/No」欄を選択してください。 「Yes」の場合、本人確認のためにどのような要素を用いているかを記述回答欄に記入してください。	リモートアクセス端末あるいは利用者の認証においては、多要素認証がサポートされているクラウドを利用する。 [利用側の施策] 極力、多要素認証を行う。 ※大学等で運用している多要素認証をサポートしている統合認証ソリューションを利用する場合は、それ経由で利用する個々のクラウドが統合認証サービスと適切に連携できるかどうかを確認するそのクラウド自体が多要素認証をサポートしているかどうかとは別に)。	Yes
				ネットワーク・通信機能	G	2	通信のセキュリティ確保	端末からサーバまでの通信のセキュリティ確保がサービスとして提供されているか「Yes/No」欄を選択してください。 「Yes」の場合、どのようにセキュリティを確保しているか、方式(SSHやSSL/TLSによる暗号化、ファイル共有におけるAES、SINET L2VPN、IPsec、SSL-VPN等)を記述回答欄に記入してください。	端末からサーバまでの通信に関して、「電子政府推奨暗号リスト」に記載された複数の暗号化アルゴリズムおよびそれに基づいた安全なプロトコルを選択することが可能なクラウドを利用する。 [追加策] VPN回線でクラウドを利用する場合、二重の暗号化を行う(例えば、インターネット VPN 回線において IPsec で通信経路の暗号化を行った上で HTTPS 通信によりコンテンツの暗号化を行 う)などを考慮する。	Yes
				ネットワーク・通信機能	G	8	IPアドレス制限の可否	ユーザはアクセス元のIPアドレスをもとにアクセス制御を行うことはできるか「Yes/No」欄を選択してください。	アクセス元のIPアドレスに基づいてアクセス制御を行うことの可能なクラウドを利用する。 [利用側の施策] ネットワークセグメントの分割を適切に設計・設定することによりアクセス制御を行う。	Yes
				データ管理	M	1	ログの知的財産権	アプリケーションログ(SaaS、IDaaS)あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ(IaaS)の知的財産権がクラウド事業者とユーザ(または契約大学)のいずれに帰属するか、契約書や約款等に明記されているか「Yes/No」欄を選択してください。 「Yes」の場合、契約大学・研究機関が文書を閲覧する方法(ウェブページに掲載、契約時に書面交付など)を記述回答欄に記入してください。	必要なログを取得するために、ログの知的財産権が利用者に帰属するクラウドを利用する。	Yes
				データ管理	M	2	ログの使用権(閲覧等)	アプリケーションログ(SaaS、IDaaS)あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ(IaaS)の使用権(閲覧等)がユーザ(または契約大学・研究機関)に認められているか「Yes/No」欄を選択してください。 「Yes」の場合、閲覧できるログの種類を記述回答欄に記入してください。さらに閲覧するログをユーザがダウンロードして保管することが可能であれば記入してください。	必要なログを取得するために、利用するクラウドのログの使用権(閲覧等)が認められているクラウドを利用する。 [追加策/要件に応じて検討] 利用するクラウドの時刻設定が可能な場合には、タイムサーバなどを利用して基準となる時刻に同期させる。また、ログに時刻情報も記録されるように設定する。 データにアクセスした利用者を特定できるようなアクセスログを取得できるように設定する。 データベースの操作ログを取得できるように設定する。 VPN回線を利用してクラウドを利用する場合、主体認証ログを取得できるように設定し管理する。	Yes
				データ管理	M	3	ログの使用(閲覧等)可能期間	アプリケーションログ(SaaS、IDaaS)あるいはクラウド事業者が管理するサーバのシステムログ/操作ログ/アクセスログ(IaaS)の使用(閲覧等)の可能期間が定められているか「Yes/No」欄を選択してください。 「Yes」の場合、可能期間を記述回答欄に記入してください。また、大学・研究機関からの要請により、可能期間を延長または短縮することが可能な場合には、記入してください。	[利用側の施策] 利用するクラウドのログの使用(閲覧等)の可能期間を確認し、大学等で定めたログの保存期間中はログを管理できるようにする。サービスにおけるログの使用可能期間が大学等で定めた保存期間より短い場合には、ログをログサーバ等に保管し、定めたログの保存期間中はログを閲覧できるようにする。	Yes/No

		208	D2101-208 (サーバ装置及び情報ネットワーク資源の管理)(p.213) 第二百八条 部局技術責任者は、サーバ装置及び情報ネットワークの利用を総合的かつ計画的に推進するため、サーバ装置の CPU 資源及びディスク資源並びにネットワーク帯域資源を利用者等の利用形態に応じて適切に分配し管理すること。	管理機能	H	2	稼働状況の一覧表示機能	ユーザに割り当てられたプロセスの死活やリソースの使用率などのサービス稼働状況を一覧で表示する機能は提供されるか「Yes/No」欄を選択してください。	サービス稼働状況やネットワーク状況を確認できる機能が提供されているクラウドを利用する。 [利用側の施策] その機能を使用して運用状況を確認・記録し、それに基づいてサーバやネットワークの資源を適切に分配・管理する。	Yes
				管理機能	H	9	プロセス監視機能	ユーザに割り当てられたプロセスの死活やリソースの使用率の監視・アラート機能は提供されるか「Yes/No」欄を選択してください。	プロセスの監視・アラート機能が提供されているクラウドを利用する。 [利用側の施策] 当機能によって状況を確認し、サーバやネットワークの資源を適切に分配・管理する。	Yes
				管理機能	H	11	利用統計	サービスへのアクセス数やリソースの利用率など、利用統計を取得する機能は提供されるか「Yes/No」欄を選択してください。 「Yes」の場合、どのような統計が取得可能か記述回答欄に記入してください。	利用統計を取得できるクラウドを利用する。 [利用側の施策] 当機能によって通信回線の通信量、接続率等の運用状態を定常的に確認・記録・分析し、サーバやネットワークの資源を適切に分配・管理する。	Yes
				スケーラビリティ	J	1	スペックレベル選択	ユーザがニーズに応じたサーバ構成を容易に選択できるように、CPUやメモリ、ストレージ等の初期構成を複数のメニューから選択することができるか「Yes/No」欄を選択してください。	スペックレベルの選択が可能なクラウドを利用する。 [利用側の施策] 当機能によって利用者等の利用形態に応じて適切な構成を選択する。	Yes

国立情報学研究所　クラウド支援室
https://cloud.gakunin.jp/
Mail: cld-office-support@nii.ac.jp