



大学・研究機関のための クラウドスタートアップガイド

パブリックレビュー Ver.1.0 (2016/9/20)

国立情報学研究所 クラウド支援室

1. はじめに

本ガイドラインは、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（以後、「大学等」と表記）の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ものである。

クラウドには、迅速性や柔軟性、運用・経済負担軽減等の様々なメリットがある一方で、導入時には、安全性や信頼性、契約方法など、サーバを購入する場合とは異なる条件を考慮して検討を進める必要がある。国立情報学研究所では、クラウドの導入・活用に関わる情報を大学等の間で共有することを目的として「学認クラウド 導入支援サービス」を実施している。

本ガイドラインでは、「学認クラウド 導入支援サービス」が提供するクラウド導入のためのチェックリストを活用してクラウドを導入する方法やそのケーススタディを紹介する。

本ガイドラインの構成は以下のとおりである。

1. はじめに
 2. クラウドとは
 3. クラウドの導入
 4. 大学・研究機関におけるクラウド利用料の支払い方法
 5. ケーススタディ：オンプレミスからクラウドへの移行
- 付録1 用語集
付録2 大学・研究機関におけるクラウド導入・利用の課題
付録3 NIIのクラウド関連サービス



2. クラウドとは

2.1 クラウドの定義とその特徴

クラウドコンピューティングを一言で説明するならば、「雲(ネットワーク)の向こう側に存在する計算機資源を、ネットワーク経由で必要なとき必要なだけ利用するサービス」であると言える。

クラウドの定義

厳密な定義としては、ISOによって、国際標準として定められている※1 共用の物理または仮想資源の**拡張可能かつ柔軟性のある集積に対するネットワークアクセス**を可能とするパラダイムであり、**必要に応じたセルフサービスの割当て**と管理を伴う。

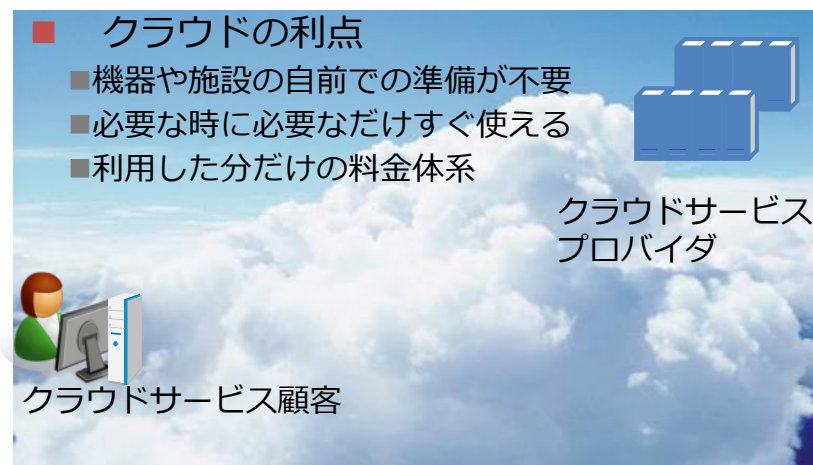
注) 資源の例として、サーバー、OS、ネットワーク、ソフトウェア、アプリケーション、ストレージ装置を含む。

クラウドの特徴

さらに、ISOでは、この定義に沿って、以下の特徴をあげている。

- 広範囲の**ネットワークアクセス性**: いろいろなクライアント(パソコン、タブレット、スマートフォン)などから、標準的なしくみで**ネットワークを通じて使用**できる。
- **計測性**: サービスの利用が監視でき、制御でき、報告され、課金される。
→ **使用した分だけの料金支払い**(従量課金)とサービスの透明性が実現される。
- **オンデマンド、セルフサービス性**: ユーザ自身が、**必要に応じて**、利用する資源を増減できる。
- **迅速・柔軟性、拡張性**: 無限のように見える資源を、時には自動的に、**柔軟に迅速に増減**できる。
- マルチテナント性: 利用者(群)に割り当てられた資源は他の利用者(群)に見えない。
- 資源のプール化: 資源は集約され利用者間で共有される。
→利用者は資源がどのように管理されているか知らなくてよい

逆に、これらの特徴を満たすサービスが、真にクラウドらしいサービスであるということもできる。



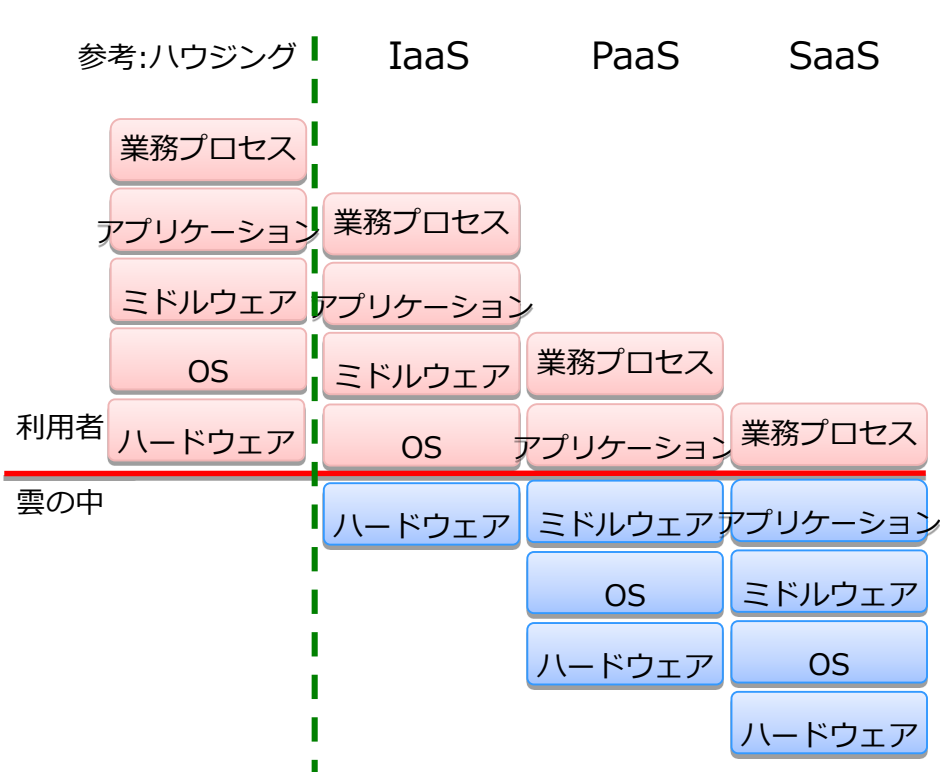
※1 ISO/IEC 17788 Information technology – Cloud computing – Overview and vocabulary (2014)、一部修正

2.2 クラウドのサービスカテゴリ

提供される資源や機能によるカテゴリ

- Software as a Service (SaaS)
クラウド内のサーバ上で実行されるアプリケーション(ソフトウェア)を提供するサービス
- Platform as a Service (PaaS)
クラウド内で動くアプリケーション (ソフトウェア) の開発・実行環境を提供するサービス
- Infrastructure as a Service (IaaS)
クラウド内の(多くの場合は仮想化された)計算機を提供するサービス

それぞれのカテゴリにおける利用者とクラウドサービスプロバイダとの責任範囲を図に示す。






特定の資源や機能を提供するクラウドサービスカテゴリ

- DaaS (Desktop as a Service)
リモートデスクトップの機能を提供
- DSaaS (Data Storage as a Service)
ストレージ容量およびアクセス・管理機能を提供
- DBaaS (DataBase as a Service)
データベースのアクセスおよび管理機能をオンデマンドに提供。データベースの構築や運用管理などの作業はサービスプロバイダが実施する。
- IDaaS (IDentity as a Service)
アイデンティティやそのアクセス権限の管理 (Identity and Access management, IAM) 機能を提供するサービス。既存の運用環境を含めて集中管理することができる。ディレクトリやシングルサインオンの機能なども提供される。

2.3 クラウドの配備モデル

代表的な配備モデル

配備モデル(deployment model)とは、クラウドサービスを実現するIT基盤がどのように提供されるかを整理したものである。

	概要	アナロジー
パブリッククラウド	サービスが不特定多数の顧客に提供され、資源はクラウドサービスプロバイダによって統制される。	公共交通機関 
プライベートクラウド	サービスが特定顧客専用提供され、資源はその顧客によって統制される。	貸切バス 
[参考] オンプレミス	資源を顧客自身が所有し顧客の施設に設置し顧客自身が維持・管理を行う。	社有車 

この他に、以下の用語もしばしば使われる。

- コミュニティクラウド: 共通の目的を持つコミュニティ(研究コミュニティ等)向けのクラウド
- ハイブリッドクラウド: 上記を複数組み合わせ合わせて利用する形態
[「オンプレミス」を除いた用語の定義はISO/IEC 17788に準拠]

プライベートクラウドを実現するパターン

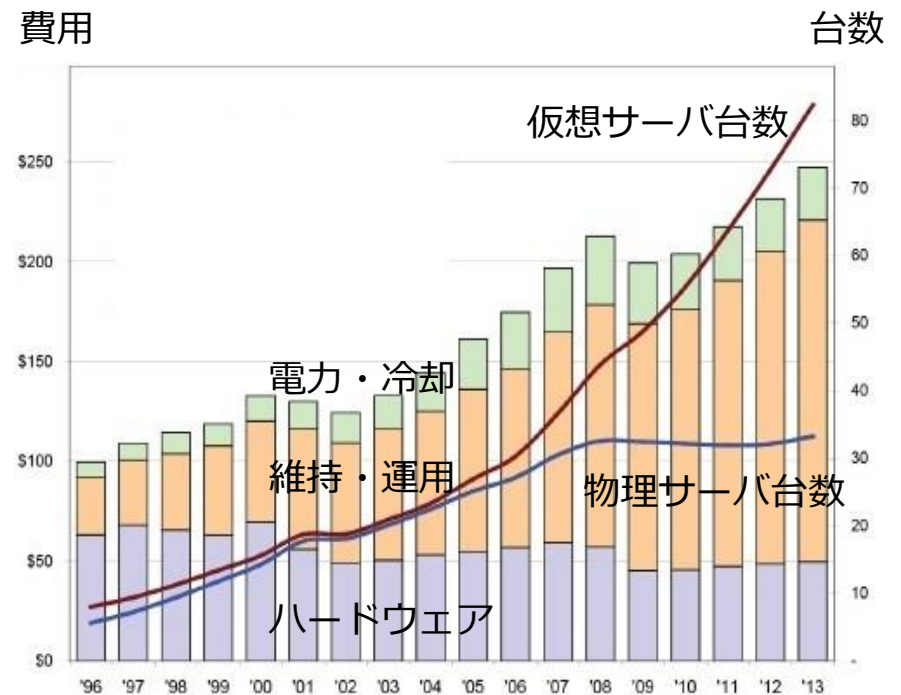
厳密には、プライベートクラウドには、以下のパターンがある。

- 顧客外部のサービスプロバイダによるサービスとして提供される場合(アナロジー: バス会社の貸切バス)
 - パブリッククラウドの一部の資源を特定顧客が専有利用することができるサービス
 - サービスプロバイダが特定顧客専用の資源を顧客の施設に設置し、リモート運用を行うサービス など
- オンプレミス型で顧客自身が所有する資源を用いたサービスを顧客の属する組織に対して提供する場合(アナロジー: マイクロバスと運転手を社有)

2.4 クラウドの利点(1)

情報システムの整備・運用が抱える課題

- インフラストラクチャ維持・運用コストの増大
 - IT費用の60%はインフラストラクチャの維持・運用費に使われているとの調査結果もある。[IDCの調査結果(2012)]→右図
- IT資源が十分活用されていない
 - 全世界のサーバ30万台中75%は5%以下の負荷でしか運用されていないという調査結果もある。[The Green Gridの調査結果(2009)]
- システムの配備・拡張のスピードが求められている。
 - 変化への即時対応により機会損失をなくすることが目標となっている。研究のためのIT基盤としては、たとえば、生まれたアイデアをいかに速く計算機を使って検証できるかといったことが求められる。



[出典: IDC 2012]

これらの課題の解決や軽減のために、これまでに述べた特徴を持つクラウドが重要な選択肢となる。

2.4 クラウドの利点(2)

クラウド導入の効果

前ページで述べた情報システムの課題に対して、クラウド導入によって得られる効果は、以下のとおりである。

	クラウド	オンプレミス (従来)
迅速性・柔軟性の実現	<p>すぐに利用(構成変更も)できる。</p> <ul style="list-style-type: none"> ✓ ハードウェア (やソフトウェア) の購入・設置 (設定) が不要。 ✓ 数分でサーバの導入や構成変更が可能。 	<p>サーバ購入・設置に数日～数ヶ月必要。</p> <p>→利用開始の遅れ 機会損失</p> 
最新技術への追随	<p>常に最新のサーバを利用できる。</p> <ul style="list-style-type: none"> ✓ 契約期間中でも新型サーバに移行可能。 ✓ 最新機能 (例: GPU, SSD) の追加も可能。 	<p>契約期間 (耐用年数) は同じサーバを利用。</p> <p>→技術の陳腐化</p> 
運用負担の軽減	<p>サーバ(ハード)の保守・障害対応不要</p> <ul style="list-style-type: none"> ✓ 障害時はクラウド事業者が (自動的) に復旧。ユーザへの影響最小。 ✓ 電気設備点検の停電対応不要。 ✓ セキュリティ対策負担軽減・徹底 	<p>ハードウェア保守・障害対応のための業務負担大。</p> <p>→教職員業務圧迫</p> 
経費負担の削減	<p>使った分だけ支払う</p> <ul style="list-style-type: none"> ✓ 従量課金 (10分単位～) ✓ 光熱費負担軽減、サーバ室設備整備不要 	<p>繁忙期に合わせたサーバの購入が必要。</p> <p>→費用増大</p> 



3. クラウドの導入

3.1 クラウド導入への流れ

クラウド導入のための作業

大学等がクラウドサービスを導入する際には、機関内で下図に示す複数段階の作業が必要となることが想定される。これらの作業は、あるサービスを調達する際、クラウドサービスを導入（クラウド化）するべきか否かという段階から始まり、大学等の要件定義、要件を満たすようなクラウドサービスの調査、仕様の検討等からなる。

NIIの支援

国立情報学研究所（以下「NII」）クラウド支援室では、下図に示すように各作業に対する支援を実施している。

クラウドサービス導入の検討段階では本資料（スタートアップガイド）やNIIクラウド支援室が定期的に開催しているクラウド利活用セミナーが参考となる。大学の要件定義では「3.2 学認クラウド導入支援サービス」で紹介するチェックリストのクラウド事業者による回答や本資料が参考となる。

クラウドサービスの調査、仕様検討の各作業においてはチェックリストの回答が活用できる。また、すべての作業について、必要に応じて大学等とNIIの間で個別相談を行っている。

調達で想定される各作業において利用可能なサービス

	チェック リスト 回答	スタート アップ ガイド	セミナー	個別相談
クラウドサービス 導入の検討		✓	✓	✓
大学の要件定義	✓	✓		✓
クラウドサービスの調査	✓			✓
仕様検討	✓			✓
調達				

3.2 学認クラウド 導入支援サービス(1)

大学・研究機関におけるクラウド導入の課題を解決

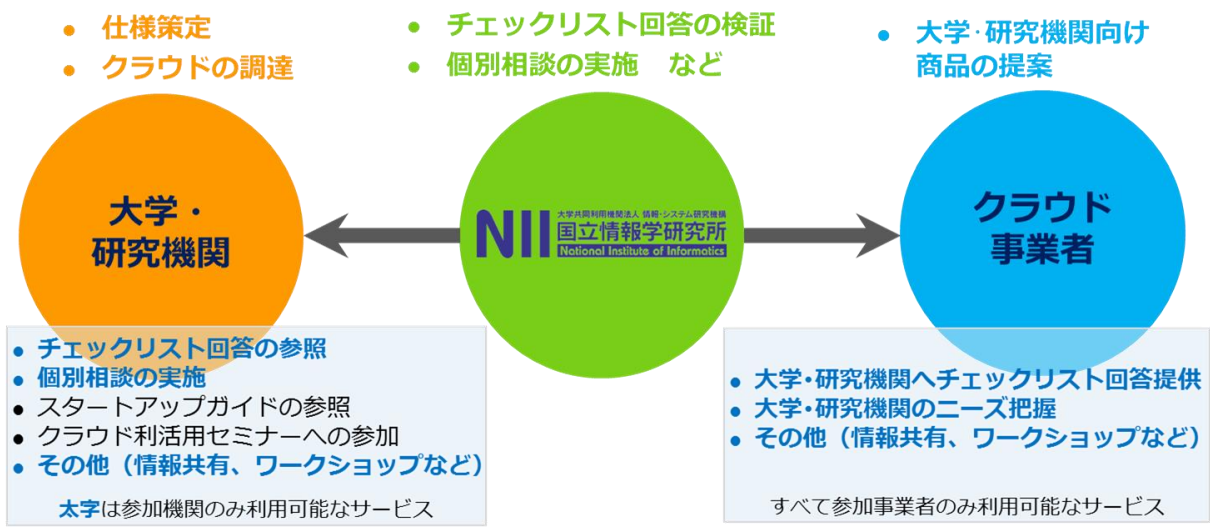
NIIが推進する「学認クラウド 導入支援サービス」は、大学等がクラウドを選択する際の基準やその導入・活用に関わる情報を整備・流通・共有するしくみである。

大学等のクラウドサービスの導入・利用における大きな課題として、クラウドを導入する際の仕様策定が困難であることが挙げられる。クラウドの導入にあたっては、技術的な機能要件から、性能・信頼性などの非機能要件、さらに契約条件など多岐に渡る項目を考慮しなければならない。

クラウドサービスの仕様策定にはこれらの要件・項目について選択基準を明確にし、事業者から提供されている多くのクラウドサービスの中から大学等の業務のニーズに合うサービスを探し出す必要がある。さらに、クラウドサービスは「サービス商品」であることから、契約・約款・SLA (Service Level Agreement) などの手続きや法律の領域に踏み込んだ検討も必要である。

「学認クラウド 導入支援サービス」では、下図に示す大学等とクラウド事業者を結ぶ枠組みを作ることにより、これらの課題を解決し、大学等における仕様策定や比較検討の負担を減らして、ニーズに合うクラウドを調達できるように支援する。

学認クラウド 導入支援サービス  GakuNin Cloud <http://cloud.gakunin.jp>

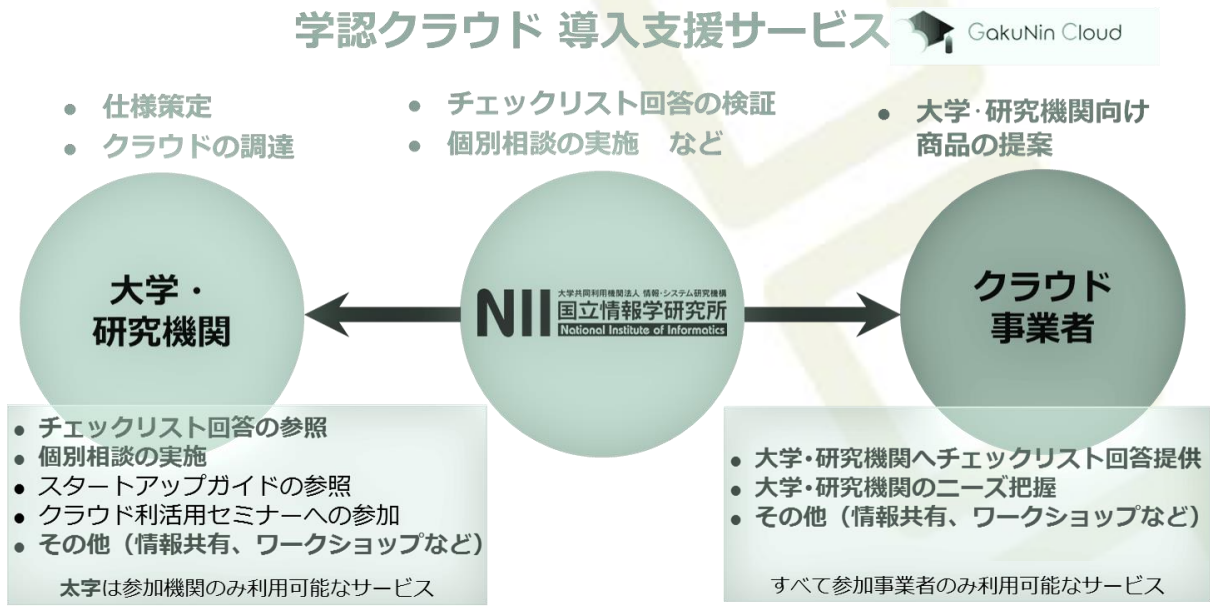


3.2 学認クラウド 導入支援サービス(2)

チェックリスト

チェックリストを用いた導入支援サービスは、以下のように進められる。

1. NIIがクラウド導入・選択のためのチェックリストを策定する。これはクラウドを導入する際の選択基準や考慮点となる項目を一覧表としてまとめたものである。
2. クラウド事業者は、自社のクラウドサービスにおいて、これらの項目に関して何がどのように提供されているかをチェックリストに記入する。
3. 記入済のチェックリストをNIIが検証した上で、大学等に提供する。
4. 大学等は、チェックリストの情報を活用して、クラウドの調達を行う。



3.3 チェックリストを用いた仕様策定

チェックリストの構成

導入支援サービスで用いるチェックリストの構成を右に示す。チェックリストはクラウドの調達の際に考慮すべき点を網羅的にまとめたものであり、サービスの種類によってはチェックリスト内のいくつかの項目について「未対応」や「対応不可」とするクラウド事業者からの回答も存在する。

チェックリストの利用方法として、このような回答が含まれるサービスを無条件に調達の候補から除外するのではなく、大学の求める要件に対応した項目がどれであるかを大学自身が判断し、それらの項目の回答を調達の参考として仕様書を作成するというような利用方法を想定している。

最新のチェックリスト（Ver. 2.0）の項目は18種類のチェック項目（大項目）に分類される。それぞれの大項目は複数の詳細チェック項目を含み、合計で116種類の詳細チェック項目が用意されている。

チェック項目（大項目）	詳細チェック項目数	主な詳細チェック項目
商品 / サービスの概要	4	タイトル、製品概要など
運用実績	2	契約法人数、運用年数
契約申込み	12	支払方法、ライセンス体系など
学認対応状況	2	Shibboleth利用可否、学認対応状況
信頼性	7	サービス稼働率の実績、計画停止の頻度など
サポート関連	5	サポート窓口、サポート回答時間など
ネットワーク・通信機能	9	SINET接続状況、通信の暗号化可否など
管理機能	11	稼働状況の一覧表示ツール、利用統計など
動作保証	3	利用可能OS、動作事例など
スケーラビリティ	6	資源の上限、作成可能なサーバ上限数など
データセンター	8	防犯設備、データの保存場所など
セキュリティ	10	セキュリティ対策、インシデント対応など
データ管理	10	データの多重化、ログなど
バックアップ	6	バックアップサービスの有無、リストアなど
クラウド事業者の信頼性	6	第三者認証、委託先での個人情報保護など
契約条件	6	責任範囲の明確化、損害賠償責任など
データの取り扱い	5	データの所有権 / 利用権、削除の方法など
データの引継ぎ	4	契約終了時の移行支援、イメージの移行性など

チェックリスト公開URL <http://cloud.gakunin.jp>

3.3.1 チェックリストの読み方(1)

商品／サービスの概要・運用実績

クラウドサービスの導入検討時には、サービス内容だけでなく、（大学等における）利用実績も導入検討の参考になる。

契約申し込み

クラウドサービスの支払い方法や課金体系は多様であり、組織の会計手続きで対応可能かを検討しておくことが必要である。無料の試用（トライアル）サービスを設けているクラウド事業者もあり、これらのサービスの利用は導入検討の参考になる。

参考：課金の留意点

【課金の期間】

同じクラウド内でも、サービスや利用する機能によって異なることがあるので、注意を要する。

- 課金の単位期間
年単位、月単位、日単位、時間単位、分単位
- 課金単位の期間に満たない利用期間の取扱い
課金単位期間の中途からの利用開始・利用終了の取扱い
(切上げ/切捨て/月単位の場合の日割計算など)

【実際の請求期間】

- 月払い、年払い
- 一括払い、分割払い、
- 先払い、後払い

参考：各種のディスカウント

- ボリュームディスカウント
一定量以上の資源を利用する場合は、利用量に応じたディスカウントが得られることがある(単価の低減、総額の一定パーセンテージの割引、など)
- 資源の予約利用
クラウドサービスによっては、同一資源を一定期間に渡って使い続けるサービスを利用し、その課金を一括で先払いするとディスカウントが得られることがある。クラウドの特徴であるオンデマンド性には反するが、既存システムの移行などで資源の利用量があらかじめわかっている場合などには活用できる。

3.3.1 チェックリストの読み方(2)

学認対応状況

学術認証フェデレーション（学認）に参加している大学等では、クラウドサービスの学認への対応状況（今後の対応予定も含む）は導入検討の参考になる。

信頼性

クラウドサービスでは、システム保守のための計画停止や障害等による計画外停止に関する情報をクラウド事業者が持つため、これらの情報の利用者への通知方法を確認することが必要である。

多くのクラウド事業者では、Service Level Agreement (SLA) を示しており、サービスの信頼性に関する指標として導入検討の参考になる。

大学等が利用するクラウドサービスが事業者の事情（事業撤退等）で終了してしまうと、非常に影響が大きい。事業継続性に関する第三者認証を取得しているクラウド事業者もあり、事業継続に関する指標として導入検討の参考になる。

参考：SLA

SLA とは、クラウドサービスを提供するプロバイダと顧客の間に締結される合意書であり、サービスの定義、範囲、内容、品質、達成目標などを規定する。一般に、SLAは以下のような内容を含む。

- SLAの目的
- SLAの範囲及び責任
- SLAの改訂方法
- SLA対象となるサービス
- サービスレベルの項目
- サービスレベルの測定手段・報告方法
- サービスレベルの目標
(Service Level Objective : SLO)
- SLO未達時の賠償、賠償要求プロセス
- SLOや賠償が適用されない例外事項

クラウドサービスのSLO未達時の賠償は、利用料金の一部返還(無料化)に留まることが多い。

SLAの項目は多岐に渡るが、代表的なものとして、以下のようなものがある。

- 可用性、信頼性
- 性能
- 資源の追加
- セキュリティ
- サポート
- データの保護(バックアップ、リプリケーション、災害対策、格納地域) など

3.3.1 チェックリストの読み方(3)

サポート関連

クラウドサービスでは、システムの状態やサービスに関する情報をクラウド事業者を介して取得する必要があるため、クラウド事業者のサポート体制について確認することが必要である。

ネットワーク・通信機能

クラウドサービスでは、学外のデータセンターのサーバを利用するため、大学等とデータセンター間の通信の安全性および性能を確認することが必要である。また、サーバへのグローバルIPアドレス割当ては、クラウド事業者によって異なるため、大学等の運用との整合性を確認することが必要である。

管理機能

クラウドサービスのユーザやサーバ管理を利用者が実施する場合は、これらの管理ツールを確認することが必要である。ロードバランサやフェイルオーバー等の機能を提供するクラウド事業者もあり、サーバの安定運用を実現する手段として導入検討の参考になる。

参考：インシデント発生時の対応

インシデントが発生した場合、原則として、大学等で定められているインシデント対応に関するポリシーに従った対応を取る必要がある。その実施において、クラウド事業者との連絡窓口や情報共有の方法確認しておくことが必要である。

参考：SINETクラウド接続サービス

NIIでは、SINETに商用クラウドを直結する接続環境を提供しており、大学等から商用クラウドサービスを高速・安全・低価格で活用することが可能となる。

詳細は <https://www.sinet.ad.jp/> を参照。

3.3.1 チェックリストの読み方(4)

動作保証

オンプレミス型のサーバ上で利用しているソフトウェアをクラウドサービス上で利用する場合は、ソフトウェアの動作保証や実績について確認することが必要である。

スケーラビリティ

クラウドサービスのメリットの一つは、サーバの仕様や数を動的に変更できる（スケーラビリティ）ことである。これらの機能を確認することは、スケーラビリティを必要とする運用では、これらの機能を確認することが必要である。

データセンター

クラウドサービスの信頼性や安全性を判断するために、サーバが設置されるデータセンターの仕様（安全対策等）を確認することが必要である。データセンターに関する第三者認証を取得しているクラウド事業者もあり、導入検討の参考になる。

また、データの保存については、保存場所（国や地域）の確認や保存場所指定の可否を確認することが必要である。

3.3.1 チェックリストの読み方(5)

セキュリティ

クラウドサービスでは、提供されるサービスに関わるセキュリティ管理はクラウド事業者が責任を持つため、クラウド事業者のセキュリティポリシーや対策を確認することが必要である。セキュリティに関する第三者認証を取得しているクラウド事業者もあり、導入検討の参考になる。

また、クラウドサービスでは、複数の利用者（組織）がサーバ等の資源を共有する場合があるため、資源分離のレベル（複数ユーザの仮想マシンが同一の物理サーバを共有等）を確認することが必要である。

データ管理・バックアップ

クラウドサービスでは、データはクラウド事業者が管理するサーバに保存されるため、データの多重化やアクセス制限、バックアップ等について確認することが必要である。

また、クラウドサービスに関するログはクラウド事業者が管理するため、利用者によるログの利用方法について確認することが必要である。

参考：情報の格付けとクラウドサービス

大学等で下の例のような情報の格付けやその取り扱いに関するルールが定められている場合、区分に応じてクラウドサービスを選定する必要がある。

機密性についての格付けの定義

格付けの区分	分類の基準
機密性3情報	本学で取り扱う情報のうち、秘密文書に相当する機密性を要する情報
機密性2情報	本学で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、その漏えいにより利用者の権利が侵害され又は本学活動の遂行に支障を及ぼすおそれがある情報
機密性1情報	機密性2情報又は機密性3情報以外の情報

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 C2103 情報格付け基準, 国立情報学研究所, 2016年

3.3.1 チェックリストの読み方(6)

クラウド事業者の信頼性・契約条件

クラウド事業者の信頼性を確認するため、経営状況や監査等の情報は、導入検討の参考になる。

クラウドサービスの利用は、利用契約に基づいて提供されるため、準拠法や管轄裁判所等の契約条件を確認することが必要である。特に、クラウドサービスでは、クラウド事業者が責任を持つ部分と利用者が責任を持つ部分があるため、両者の責任範囲を確認することが必要である。

参考：契約の構成要素

クラウドサービスの契約には、一般的には、以下のような構成要素が含まれる。

- ・ サービス内容説明
- ・ 利用規約
- ・ SLA
- ・ セキュリティポリシー/個人情報保護ポリシー/知的財産権ポリシー
- ・ 価格、料金支払条件、料金支払方法
- ・ 免責事項
- ・ 契約解除・更改・契約内容変更・サービス終了手続

これらがどこまで文書化されているか、どのような文書体系となっているか、どの文書に何が書かれているかはプロバイダによって異なる(例、セキュリティポリシーは単独文書またはSLAの一部に記述)。

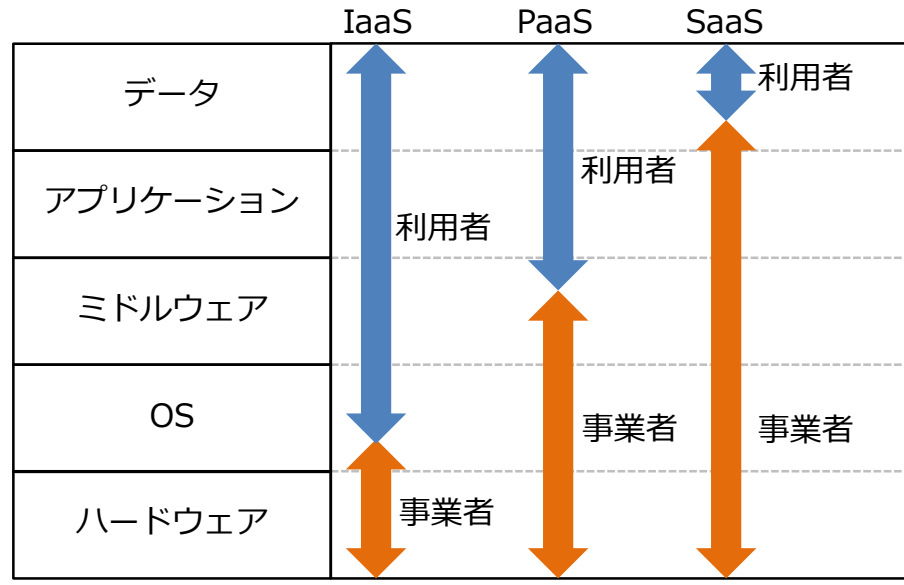
参考：クラウド事業者と利用者の責任範囲

クラウド事業者と利用者の責任範囲は、例えば右図のように、サービスカテゴリによって異なることが一般的である。

例えば、右図のIaaSの例では、仮想化基盤を含むハードウェアおよびVM作成時のOSのセキュリティ対策はクラウド事業者が責任をもち、それら以外は利用者が責任を持つことを示している。従って、VM作成後のOSへのセキュリティパッチ適用等は利用者の責任となる。

【注意】 右図に書かれた責任範囲はその一例であり、実際の責任範囲はクラウドサービスによって異なるため、導入時によく確認すること。

クラウド事業者と利用者の責任範囲（一例）



3.3.1 チェックリストの読み方(7)

クラウド事業者の信頼性・契約条件(続)

参考：約款や利用規約への同意

約款ベースのパブリッククラウドの場合、サービスの利用開始やダイアログボックスへのチェックなどの簡単な手続きをもって、契約条項に同意したとみなされる場合が多い。しかし、約款や関連文書の中には、たとえば知的財産権などに関する重要な条項が記述されていることもあり、場合によっては、利用開始前に法務の専門家を含めた確認が必要となる場合もある。上記の契約の構成要素の多くはWeb等で公開されているので、事前のチェックが可能である。

参考：約款による契約

クラウドサービスによっては顧客と個別契約を締結する場合もあるが、多くのパブリッククラウドサービスでは、特定多数の利用者を想定して、定型的に処理できるあらかじめ作成した契約条項、すなわち約款による契約であることが多い。

データの取り扱い・引き継ぎ

クラウドサービスでは、データはクラウド事業者のサーバ上に保存されるが、データの所有権は利用者にあるべきである。そのため、データ所有権、および契約終了時のデータやアカウント情報の取り扱いについて確認することが必要である。

また、他の事業者のクラウドサービスへ利用を移行する場合は、データ等の移行支援に関する情報が、導入検討時の参考になる。

参考：ベンダロックイン

サービスを継続的に利用することに伴い、そのサービス特有の機能への依存が大きくなり、他のクラウドサービスに乗り換えることが難しくなる状況（ベンダロックイン）が起こりえる。ベンダロックインが起こりにくいクラウドサービスを導入することは、より良いクラウドサービスを効率よく利用することにつながる。



4. 大学・研究機関におけるクラウド 利用料の支払方法

4.1 支払方法の選択基準

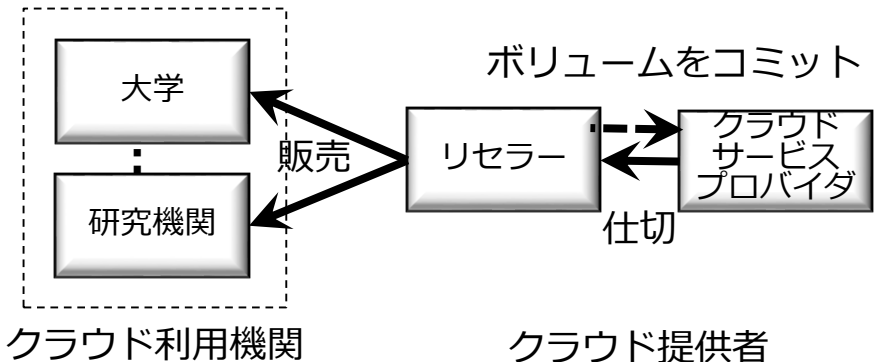
請求書払いとクレジットカード払い

クラウドサービス利用料の支払方法には、請求書払いとクレジットカード払いがあり、どの方法が可能かはプロバイダによって異なる。また、利用料が高額となる場合には、入札による調達が必要である。

- 請求書払い
大学等における一般的な支払方法であり、通常の支払手続きで処理できることが多い。
- クレジットカード払い
パブリッククラウドでは、クレジットカード払いしか受け付けないプロバイダもあるが、クレジットカード払いは、大学等の場合、会計・支払制度に適合しない場合も多い。したがって、クレジットカード払いの場合は、以下のいずれかの対応となる。
 - ✓ 代理店を利用して、請求代行あるいはバウチャー購入による請求書払いとする。
 - ✓ 大学等によっては、クレジットカード払いが可能であったり、個人のクレジットカードで立替え払いすることが可能な場合もあるので、会計担当部署に確認する。

参考：請求代行

利用者が代理店と契約し、代理店がクラウド事業者からの請求額に手数料（為替等含む）を加えて利用者に請求する。手数料は代理店によって異なる。なお、代理店によっては、プロバイダとの直接契約より安価となる場合もある(ボリュームディスカウント効果)。



参考：バウチャー購入

代理店がバウチャー(一定金額までの利用権。プロバイダによっては「オープンライセンス」などの名称で販売している)を利用者に販売し、これを利用者は前払いで購入する。資源が不足すれば、追加購入することも可能である。

4.2 入札

総価契約と単価契約

クラウドサービスの調達において、入札を行う場合の契約方法には、以下の2種類がある。

1. 総価契約

- 利用期間中の総額（総価）により入札。利用者は落札額を支払う。
- 利用期間中の資源利用量と金額を見積もる必要がある。
 - 合計金額により政府調達になる場合がある。
- 原則として、契約時に決めた利用量を超えて利用することはできない、また、利用実績が契約時の利用量を下回っても返金されない。

2. 単価契約

- 一定の資源等の利用金額（単価）により入札。利用者は資源利用量の実績に応じて利用料を支払う（従量課金）。
- この場合でも、利用期間中の資源利用量と金額を見積もる必要がある。
 - 合計金額により政府調達となり、プロセスに時間を要する場合がある。

クラウドの調達については確立した方法がまだないので、所属機関の会計担当部署との相談が必要です。



5. ケーススタディ：オンプレミスからクラウドへの移行

5.1 クラウド移行効果の評価

移行前後のコスト比較を行って、クラウド導入によるコスト低減効果を評価する。評価は、以下の観点で行う。

比較対象は購入価格だけではない

- 単純にハードウェアの価格あるいは減価償却額とクラウド利用料を比較するのではなく、ある一定期間(ハードウェアの償却期間である5年間など)のTCO(Total Cost of Ownership)を比較すべきである。TCOの要素としては、以下のようなものがある。
 - ハードウェア(サーバ、ストレージ、ネットワーク機器、筐体、その他の周辺機器、記憶媒体)
 - ソフトウェア(OS、ミドルウェア、アプリケーション、ツール等のソフトウェアライセンス)
 - 保守費用(ハードウェア保守契約、ソフトウェアサポート契約)
 - ファシリティ費用(ラック費、賃貸費、電力費(ハードウェア、空調、照明、その他))
 - 運用管理費用
 - 構成管理・資産管理作業費用(棚卸等)
 - 資源配備作業費用(要求ヒアリング、要件定義、設計、キャパシティ分析・計画、移行設計、構築、構成チェック、テスト・検証、デプロビジョニング)
 - 障害対応作業費用(監視、一次対応・切分け、障害復旧)
 - セキュリティ関連作業費用(脆弱性調査、パッチ適用、セキュリティインシデント対応)
 - 機会損失(運用作業による本来の業務の阻害損失、ITインフラ展開の遅延による損失)
- クラウドのほうがTCOが高くなる場合においても、エンドユーザに対するサービス性の向上、新規サービスの提供などの要素を加味して、クラウド移行の評価を総合的に判断する。

5.2 クラウド移行にあたっての検討事項

5.2.1 性能

クラウドサービスの性能を考える上で、以下のクラウドの特徴を理解しておくことが重要である。

クラウドの本質的な特徴	実際のクラウドサービスの実装・運用からくる特徴
<ul style="list-style-type: none">ネットワーク経由でサービスを利用する。従量課金である。資源は集約されてプール化され、利用者間で共有される。	<ul style="list-style-type: none">仮想資源が提供されることが多い。x86サーバやLinuxなどのコモディティ素材が使われることが多いが、それを組み上げるアーキテクチャや実装方法は公開されずブラックボックスであることが多い。また、ブラックボックスの内容はプロバイダごとに独自であることが多い(サーバとストレージ間の接続方法など)。

これらの特徴から、クラウドで提供されるサービスや資源の性能に関しては、以下の点を考慮しておく必要がある。

- 資源のプールを他利用者と共用するため、そのふるまいが性能に影響することがある。たとえば、他利用者がネットワークに大量データを流した場合、ネットワーク性能が下がることもある。
 - 上記の理由から、プロバイダによっては、クラウドの性能値をスペックとして提示していても、その保証はベストエフォートによるものであることが多い点に注意すべきである。
 - これを避けるために、物理サーバなどを専用するオプションもある(当然料金は上がる)
- プロバイダによってアーキテクチャが異なるため、特にI/O性能に差が出ることもある。
- サービスを提供するデータセンターが遠隔地や海外にある場合、ネットワーク遅延が大きいことがある(CDN等で解消を図る場合もある)。
- IaaSではサーバスペック(コア数、性能、メモリ量)が選択可能であるが、以下の点に注意する。
 - 性能指標は、プロバイダによって異なる。
 - スペックが高いサーバほど料金も上がるため、不必要に高スペックのサーバを低い負荷率で利用することは避けるべきである(むしろスケールアップが容易なので、小さい構成から負荷を見ながら拡大してゆくことを考える)。

5.2.2 可用性

可用性の基準

クラウドサービスのSLAの一環で可用性を規定することが多い(SLAで可用性を規定しないサービスもある)。この場合、可用性は稼働率で表現されることが多い。

稼働率 = $1 - (\text{サービス停止時間} / \text{全時間})$

表に稼働率と、その値に対応する年間のサービス停止時間を示す。クラウドサービスでは、99%から99.9%程度の稼働率をSLAで保証する人が多い。

可用性は高ければ高いほど良いとは一概には言い切れない。可用性の高いサービスほど一般的に高価となるので、業務の要件に合った可用性のサービスを選択することが必要となる。

稼働率	年間停止時間
99 %	87.6 時間(3.7日)
99.5 %	43.8 時間(1.8日)
99.9 %	8.76 時間
99.99%	52.6 分

なお、サービス停止時間の定義は、プロバイダごと、あるいはサービスごとに異なる。SLAで可用性を規定している場合は、これらも文書化されているので、利用に際してはよく確認する必要がある。たとえば、

- 時間: ある一定時間以内(たとえば5分)の停止は停止とみなさない、など
- 影響範囲: 個々の顧客の資源の停止か、クラウドの全顧客の資源の停止か、など
- 機能範囲: IaaSの仮想サーバの例で言えば、仮想サーバ自体の停止か、仮想サーバに対する操作だけの停止(サーバ自体は動作を継続)か、など
- 計画停止の取扱い: 計画保守は停止時間に含めない、など

※計画停止の業務に対する影響は、導入当初から考慮しておくべきである。

ゾーンの活用

可用性に関してSLAが設定されていても、現実には、著名プロバイダにおいても、ネットワーク障害などによる大規模なサービスの中断が起きている。このような場合に備えて、同時にサービス停止が起こらない「ゾーン」という運用単位(データセンターなどに対応)を提供しているクラウドも多く、資源を配備する際には特定のゾーンを指定できるようになっている。クラウドでミッションクリティカルな業務を実施する場合は、このようなゾーンを活用した設計を行うことも考慮すべきである。

5.2.3 セキュリティ、プライバシー

利用者とプロバイダの責任分界点

利用者とクラウド事業者の責任分界点は、利用規約で規定されていることが多く、確認と利用者が行うべき対策の実施が必要である（「3.3.1 参考：クラウド事業者と利用者の責任範囲」参照）。例として、

- 仮想サーバを提供する仮想化基盤(ハイパーバイザなど)や操作のためのポータルwebサイトのセキュリティ(脆弱性対策や侵入検知)はプロバイダ責任
- 仮想サーバ上のOSやミドルウェアのセキュリティは利用者責任(プロバイダの提供するIDSサービスやマネージドサービスを購入する場合は、この限りではない)

プライバシー関連

データセンターが海外に設置されている場合があり、国外に持ち出せないデータに関しては注意を要する。

第三者認証の確認

プロバイダがデータセンターの中でどのようなセキュリティ対策や高可用性対策を行っているかは、利用者側からはブラックボックスとなっており、利用者によるセキュリティ監査も拒絶される場合が多い。一方、多くのプロバイダは第三者認証の取得や、利用者が認証を取得するための支援を行っており、これらの確認が必要となる場合がある。

第三者認証の例

カテゴリ	第三者認証
データセンター	Uptime Tier(米民間基準)、ANSI TIA-942、JDCC FS-001(日ファシリティ基準)
セキュリティ	ISO 27001(情報セキュリティ)、SOC2/SOC3(Service Organization Control2/3、セキュリティ内部統制)、FISMA(米連邦情報セキュリティマネジメント法)、PCI DSS(クレジットカード情報保護関連)、HIPAA(米医療機関における患者情報のセキュリティ)、FISCガイドライン(国内金融機関向けガイドライン)、FIPS140-2(暗号モジュールに関する米標準規格)
事業	ISO 14001(環境マネジメント)、ISO 9001(品質管理)、ISAE 3402およびSSAE 16(受託業務の内部統制保証報告に関する基準)、SOC1(財務諸表の内部統制)
その他セキュリティに関する基準	FedRAMP(クラウドセキュリティ評価/認証/監視の政府機関プログラム)、DoD CSM(米国防総省クラウドセキュリティモデル)、FDA Part 11(米食品医薬品局の電子記録基準)、CSA CAIQ(Cloud Security Alliance Consensus Assessments Initiative Questionnaire、セキュリティのドキュメンテーション基準)

5.2.4 サポート

クラウド事業者によるサポート

特に業務システムをクラウド化する場合、サポートは重要となる。サポートに関する要件は、基本的には、オンプレミスのハードウェア製品、ソフトウェア製品と同様であり、以下の諸項目を考慮する必要がある。

- どのようなサポートプランが提供されているか
- 無償サポート、有償サポート
- サポートコンタクトの方法
- 電話、電子メール、web受付、コンタクトなし(FAQや事例を自分で検索するのみ、など)
- サポート受付時間帯
- 営業時間(9am-5pmなど)、24時間365日
- サポートに対するレスポンス時間
- 第一次回答までの時間、解決までの時間
- サービス停止など重要なインシデントに関するサポート時間帯
- 障害原因・回避方法・対応策などの報告の有無
- 障害切分けの責任分界点

オンプレミスとの違い

なお、IaaSのサーバ資源の上で動作するソフトウェアに関しては、オンプレミスの場合と、サポートのレベル、環境(ソフトウェアのアップデート基盤など)、責任分界点などが異なる場合もあるので、注意が必要である。例えば、ベアメタルサーバ上で再現しないインシデントはサポートを受け付けない、など。

5.2.5 ソフトウェアライセンス

BYOL(Bring Your Own License)はベンダごとに確認が必要

ソフトウェアベンダは、これまで、オンプレミスのシステムに対するソフトウェアのライセンス販売とサポートを主なビジネスモデルとしてきた。クラウド上でのソフトウェアの利用はこのビジネスモデルを毀損する可能性もあり、現在のところ、クラウドへの展開に消極的であったり、クラウドに対する戦略を決めていないベンダも存在するのが実情である。

このような状況から、現時点では、オンプレミスのシステム用に取得したソフトウェアのライセンスをクラウド上のシステムで使用すること(BYOL)が可能であるかどうかは、各ソフトウェアベンダが任意に決めている状況にある。したがって、BYOLを行いたい場合にはベンダ個別に、ライセンス条件を確認する必要がある。特に以下のような場合もあるので、注意が必要である。

- BYOLを一切認めない場合
- クラウド上で利用できるが、使用コア数などのライセンス条件が異なる場合
 - ✓ ソフトウェアを搭載するVMに対してプロバイダが自動フェイルオーバー機能を提供している場合、フェイルオーバー対象の全物理サーバ分のライセンス取得を要求する、といったケース
- プロバイダによってクラウド上で利用できるかどうか異なる場合
 - ✓ ソフトウェアベンダが認定したクラウドサービスプロバイダに対してのみ認めるといったケース
- オンプレミスにおけるライセンス形態や契約形態によって、BYOLの可否や条件が異なる場合

5.3 クラウド移行作業

これまでオンプレミスで利用されていたアプリケーションやデータを移行する場合、以下のような複数の方法から適した方法を選ぶ必要がある。

アプリケーションの移行

オンプレミスで利用されていたアプリケーションをIaaSに移行する場合、以下のような方法が考えられる。

- 新規に配備したサーバに対して、ゼロから環境構築を行う。アプリケーションは再インストールする。
- アプリケーションを仮想サーバ上で利用していた場合、オンプレミスの仮想環境あるいは他クラウドの仮想サーバで動作していた仮想イメージを移行する。移行前後の仮想化環境(ハイパーバイザ)の組合せによって、移行できる場合とできない場合がある。移行ツールが必要な場合もある。
- Dockerなどのコンテナを利用して移行する。対象とするクラウドがコンテナのサービスを提供していることが前提となる。

データの移行

オンプレミスに保存されていたデータの移行では、以下のような方法がある。

- データをネットワーク経由で転送する。
- データ量が多く、ネットワーク経由の転送では時間がかかり過ぎる場合、クラウド事業者によっては、ハードディスクや可搬媒体(USBメモリなど)をクラウド事業者に送付することにより、クラウド事業者がこれをクラウドストレージに格納するサービスを提供している場合がある。

5.4 クラウドの利点をより多く引き出す施策(1)

オンプレミスからクラウドへの移行では、オンプレミスで利用されていたシステムを単純にクラウドに移行するのではなく、クラウドならではの機能を追加することにより、システムの高度化を実現することができる。クラウドの利点を最大限に引き出すには、移行前あるいは移行後に、以下のような施策を検討することが有効である。ただし、施策によっては、既存のアプリケーションの変更を必要とする場合も多いため、移行したシステムのライフサイクルや投資対効果を十分考慮して判断する。

スケールアウト／スケールダウン

- 最低限の資源(特にサーバ数)でシステムを立ち上げておき、負荷の増減に応じて、資源をオンデマンドに追加あるいは削減する。
- 資源の追加や削減は、手動、APIを活用したスクリプトなどによる自動化(夜間や休日の資源削減や停止)、クラウド自身が提供するオートスケールサービスによる自動化などの方法がある。
- あらかじめ、負荷状況が予測できない業務において、効果を発揮する。
- 一方、オンプレミスの低負荷率のサーバをそのままクラウドに移行した場合、低負荷率をそのまま維持したサイジングを行うと、高スペックの(=高価な)サーバを利用することになる。スケールアウトを行うことで、サーバのスペックを下げるとともに平均負荷率を向上させ、全体費用を低減することが可能である。
- アプリケーションによっては、疎結合化、ステートレス化、非同期化、リトライ可能化などの改造が必要となることがある。

既存サービスの活用

- データベースサービス(DBaaS)などの、既存サービスを最大限活用する。
- たとえば、DBaaSの場合、データベースの構築作業やバックアップなど運用管理作業の負担が軽減され、短期開発の実現や、運用管理コストの低減を図ることができる。
- アプリケーションによっては、処理とデータを分離する改造が必要となることがある。

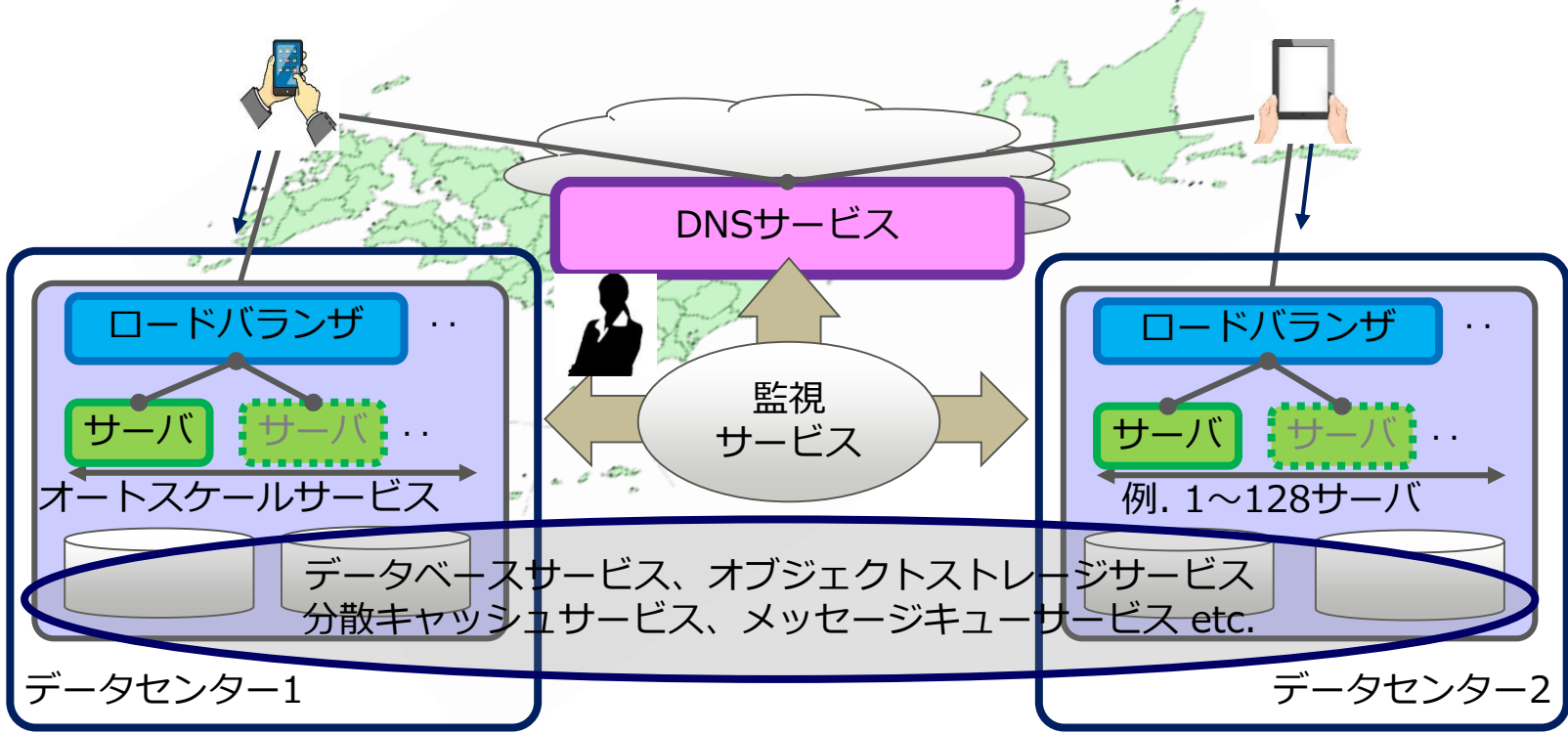
5.4 クラウドの利点をより多く引き出す施策(2)

マルチデータセンター化、地域分散化

- クラウドの資源を複数のデータセンター(ゾーン)、あるいは地域に分散して配備する。
- 災害やクラウドの大規模障害に対する回復力(resiliency)を実現できる。
- DNSの活用によって、エンドユーザに対して地域的に使いデータセンターからサービスを提供することによる性能向上を図ることもできる。

クラウドネイティブアプリケーション

以上の施策を行うことは、業務アプリケーションを、いわゆる「クラウドネイティブアプリケーション」(クラウドを前提として開発され、その特長を活用するアプリケーション)化することになる。



付録1：用語集

ここでは、スタートアップガイドおよびチェックリストの情報を活用するための参考として、クラウドに関連した用語を解説する。

英略語	英語名称
BYOL	Bring Your Own License
CDN	Content Delivery Network
DaaS	Desktop as a Service
DBaaS	DataBase as a Service
DNS	Domain Name System
DSaaS	Deep Security as a Service
DR	Disaster Recovery
IaaS	Infrastructure as a Service
IDaaS	IDentity as a Service

英略語	英語名称
LMS	Learning Management System
PaaS	Platform as a Service
SaaS	Software as a Service
SLA	Service Level Agreement
SLO	Service Level Objective
TCO	Total Cost of Ownership
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine
VPN	Virtual Private Network

用語	解説
AES	米国NISTによって制定された新しい暗号化規格。
DDoS(DoS)攻撃	ネットワーク経由で行われる外部からの攻撃の一つ。標的のコンピュータに対して大量の packets 送信で過剰な負荷をかけ、サービス提供を妨害する。攻撃元が単一の場合をDoS攻撃、複数の場合をDDoS攻撃という。
IDS/IPS	不正侵入検知システム/不正侵入防御システム。ネットワーク経由で行われる外部からの攻撃を防御する手段。ネットワーク・OS・ミドルウェアレベルでDDoS攻撃等を防御する。
IPSec	TCP/IPネットワークで安全に通信を行うためのプロトコル。暗号・認証機能を持つ。
Shibboleth	ユーザ認証方式の一つ。
SINET	日本の大学・研究機関等の学術情報基盤として、NIIが構築・運用している情報通信ネットワーク。2016年4月よりSINET5の運用を開始。
SSH	別の場所にあるコンピュータをネットワーク経由で安全に操作するためのソフトウェア。暗号・認証機能を持つ。
SSL/TLS	HTTPなど上位のアプリケーションで安全に通信を行うためのプロトコル。暗号・認証機能を持つ。
WAF	ネットワーク経由で行われる外部からの攻撃を防御する手段。Webアプリケーションレベルで不正アクセスを防御。

用語	解説
イメージ	仮想環境で実際のシステムのように動作するための構成ファイルのこと。
オンプレミス	資源を顧客自身が所有し、顧客の施設に設置し、顧客自身が管理を行うシステム。
仮想化	資源を論理的に分割・統合することで、各資源を複数の資源として利用したり、1つの資源として扱えるようにすること。
可用性	システムが正常に稼働し、必要な時にはいつでもアクセス・利用できること。
クラウド	共用可能な資源をネットワーク経由で必要な時に必要なだけ利用できるシステム。モデルとしては、ハイブリッド、パブリック、およびプライベートがある。サービスの形態としては、IaaS、IDaaS、SaaS、DaaS、DSaaS、およびDBaaSなどがある。
サイジング	システムの運用に必要な資源を見積もること。
サービス稼働率	サービス提供中、障害等でサービスが中断することなく稼働していた時間の割合。サービス中断時間がゼロの場合、サービス稼働率は100%。
資源	サービス、オペレーティングシステム、ネットワーク、ソフトウェア、アプリケーション、およびストレージ設備などのリソース。

用語	解説
スケールアウト	サーバの台数を増やしてシステムを補強すること。
ストレージ	データを記録・保存する装置。
第三者認証制度	認証の対象となるサービス事業者と利害関係のない認証機関が第三者の立場から審査し、認証を与える制度。データセンター、セキュリティ、および事業継続に関するものがある。
データ耐久性	システムがデータを失わないことの保証。
認証	ユーザがその人本人であることを証明すること。
ハイブリッドクラウド	少なくとも2つのクラウドモデルを組み合わせて利用するクラウドモデル。
パブリッククラウド	資源がネットワーク経由で不特定多数の顧客に提供され、顧客は資源を利用するが、サービス事業者が資源の管理を行うクラウドモデル。
バックアップ	ある時点のデータやファイルなどを別の装置にコピーすること。すべてのデータをコピーすることをフルバックアップ、前回との差分をコピーすることを差分バックアップという。

用語	解説
ファイアウォール	ネットワーク経由で行われる外部からの攻撃を防御する手段。ネットワーク(TCP/IP)レベルで不正アクセスを防御。
フェイルオーバー	サービス中のシステムに問題が発生した時、別のシステムに自動的に切り替わることでサービスを継続させる機能。
物理サーバ	仮想化されていない単一のサーバ。
プライベートクラウド	資源がネットワーク経由で単一の顧客に提供され、顧客が資源の利用と管理を行うクラウドモデル。
リストア	バックアップデータをもとにシステムを復旧すること。
ログ	システムで行われたイベントの履歴。
ロードバランサ	サービス利用中に発生する要求の処理先を振り分けることで負荷を分散させること。

参考：

ISO/IEC 17788 First edition | Rec. ITU-T Y.3500

情報処理推進機構 セキュリティ用語集 <https://www.ipa.go.jp/security/glossary/glossary.html>

付録2：大学・研究機関における クラウド導入・利用の課題

心理的な課題(1)

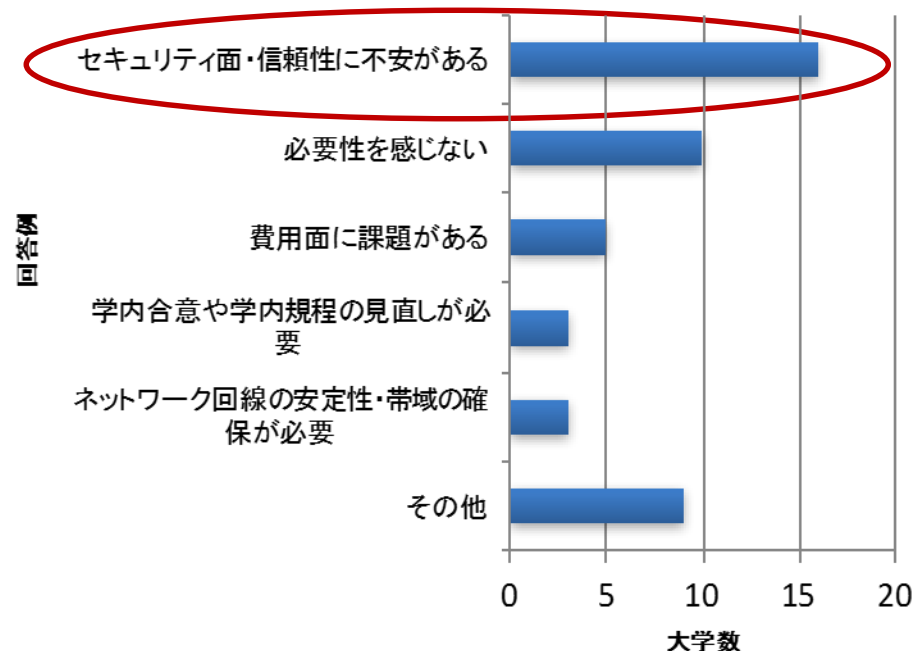
漠然とした不安

クラウドを利用することについて、漠然とした心理的な壁を感じている組織は少なくない。例えば、文部科学省による大学等に対する調査結果※1では、7割の大学がクラウドの学術利用に興味を持つ一方で、3割の大学がクラウドを利用すべきか判断できないと回答している。また、文部科学省が実施した別の調査結果※2では、右図に示すように、多くの大学がクラウドの利用についてセキュリティや信頼性に不安があると述べている。

クラウドに対する経験不足

一般に、多くの大学等では、オンプレミス型の計算機システムの導入や利用についての経験があり、知識やノウハウを蓄積している。しかし、クラウドに関する知識や、クラウドのようなサービスを導入・利用する経験が乏しいため、多くの大学等がクラウド導入・利用に関して漠然とした不安感を抱いていることが、これらの調査結果からわかる。

クラウド導入・利用の課題



※1 文部科学省, コミュニティで紡ぐ次世代大学ICT環境としてのアカデミッククラウド, 2014年

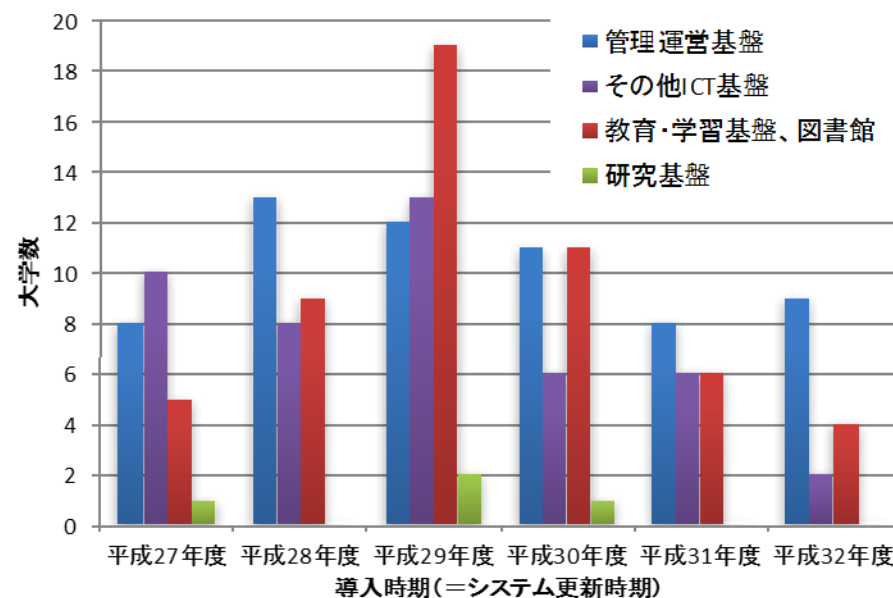
<http://www.icer.kyushu-u.ac.jp/ac/>

※2 文部科学省, クラウドコンピューティングの運用状況及び導入計画等について, 2014年

教育研究にクラウドをどのように使えばよいか わからない

また、同調査のクラウド導入予定に関する調査結果では、右図のように、管理運営基盤（主に事務系システム）でのクラウド導入が進む一方で、研究基盤（研究用の計算サーバやストレージ等）へのクラウド導入に関する計画が非常に少ないことがわかる。これはクラウド上のサーバやサービスをどのように研究や教育活動で利用するのがよいか、研究者や教育者がまだ十分に判断できていないことによると推測される。

クラウド導入予定



文部科学省，クラウドコンピューティングの運用状況及び導入計画等について，2014年

クラウドを導入するための仕様策定が難しい

大学等では、これまでの経験から、計算サーバ・ストレージ等のハードウェアやアプリケーションを導入するための判断基準はノウハウとして蓄積されているが、これらをクラウドサービスとして導入する場合の判断基準が蓄積されていない。例えば、クラウドサービスの導入では、クラウドに保存されるデータの安全性やサービスの信頼性、契約条件等についても適切に判断する必要があるが、大学等ではその判断材料が十分に蓄積されていない。



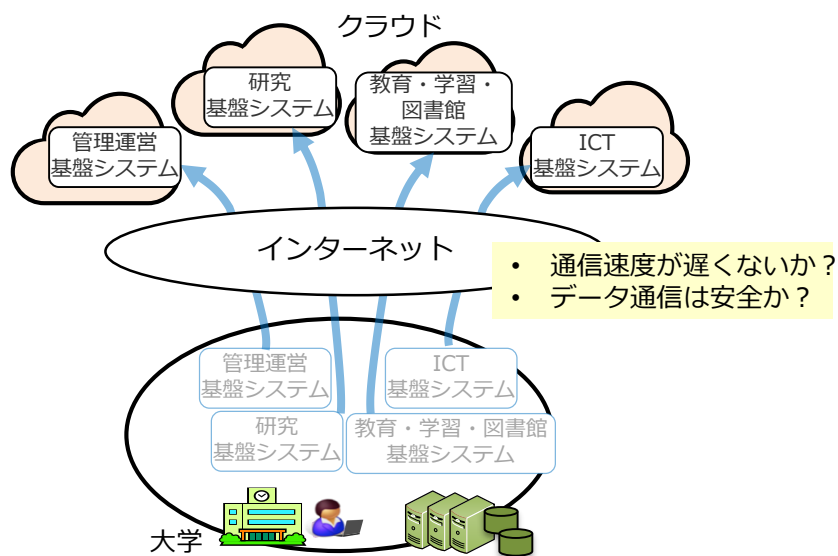
クラウドの調達ที่難しい

国立機関等では、調達手続きが課題となる。クラウドは、使いたい時にすぐに利用を開始できるとともに、利用実績に対して従量制で課金されるモデルが一般的である。しかし、入札等の手続きはこのモデルとの整合性が悪く、調達手続きによりクラウドを利用することのメリットが失われてしまうことがある。



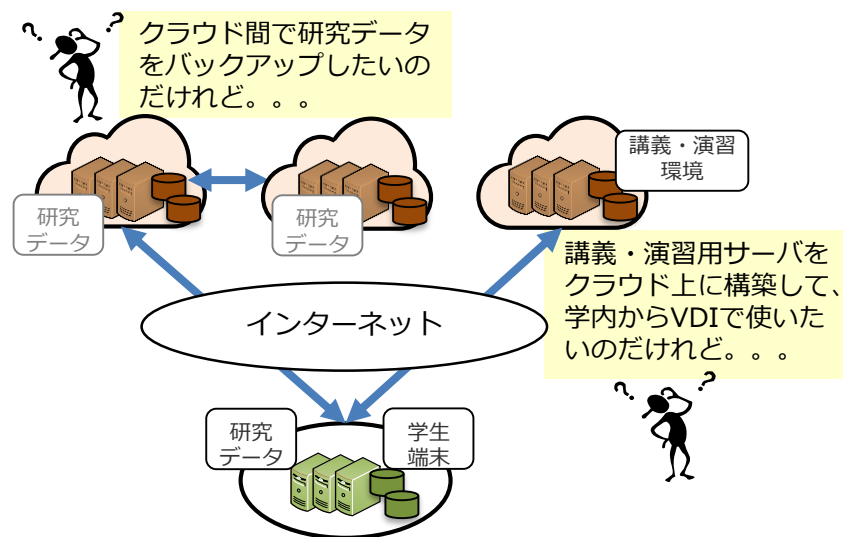
通信の応答性と安全性の確保できるか

学内の計算機システムをクラウドに移行することにより、これまで学内ネットワーク経由であった計算機システムへのアクセスがインターネット等の広域ネットワーク経由になる。そのため、クラウド移行にあたっては、学内の計算機と同等の応答性能および通信の安全性を確保できるのかという技術的な課題を解決できなければならない。



クラウド環境の構築が難しい

教育研究にクラウドを利用するためには、そのためのソフトウェアをクラウドに適切に配備しなければならないが、これには高度な知識や技術を要するため、管理者の負担が大きい。また、今後、大学の計算機システムとクラウドの併用（ハイブリッドクラウド）や、複数のクラウドを利用する方式が主流になると考えられる。複数の拠点間で計算機システムを連携させるためには、拠点間のネットワーク設定や、各拠点へのソフトウェアの配備を適切に行う必要があり、さらに環境構築が難しくなる。





付録3 : NIIのクラウド関連サービス

NIIのクラウド関連サービス(1)

- チェックリスト

大学がクラウドを導入する際の着眼点を明確にし、共通のチェック項目で複数のクラウドサービスを比較して、ニーズに合うサービス商品を探し出せるためにNIIで作成したリストのことである。

クラウド事業者は、このチェックリストに沿って自社サービスの情報提供を行うことにより、大学のニーズを把握するとともに的確なクラウド導入の提案・支援を行うことが可能になる。

クラウド事業者が記入したチェックリストをNIIで検証・評価した上で、学認クラウドサービス利用機関に提供する。

学認クラウド実証実験開始時（2015年9月）にVer.1.0を公開し、実証実験で得られた知見を反映し、2016年9月現在にVer.2.0を公開している。

- クラウド利活用セミナー

NIIで開催している研究教育におけるクラウド利活用に関して、毎回異なるシナリオを想定したハンズオンセミナーをいう。テーマの選定やハンズオンセミナーに用いるクラウド環境の利用については、毎回、クラウド事業者の協力を得て行っており、主な受講対象者は、大学等に所属する教職員、研究者、技術者、大学院生である。

- JAIRO Cloud（共用リポジトリサービス）<https://community.repo.nii.ac.jp/>

独自で機関リポジトリの構築・運用が難しい機関に対し、NIIが開発した機関リポジトリソフトウェア WEKO（<http://weko.at.nii.ac.jp/>）をベースにした共用リポジトリのシステム環境をNIIがクラウドサービスとして提供している。

NIIのクラウド関連サービス(2)

- クラウド接続サービス

SINETに商用クラウドを直結し、SINET加入機関とクラウド提供事業者間のL2VPN接続を提供するサービスである。クラウド接続においては、L2VPN方式のみが利用可能で、商用ネットワークを介さずに高速・安全・低価格で商用クラウドサービスを利用することが可能である。

- クラウドゲートウェイ

研究・教育に必要なクラウドサービスにワンストップでアクセスするためのポータル機能である。大学等の利用者はクラウドゲートウェイにログインするだけで、大学等が機関契約を行っているサービスなどに素早く、簡単に、アクセス可能となり、利用者個人でのカスタマイズ（並び順の変更、項目の追加等）も可能である。2016年より試験運用、2017年より本運用を開始する予定である。

- クラウド群連成基盤サービス（仮称）

SINET5に接続された複数のクラウド環境や大学等の計算機で構成するインタークラウド環境をオンデマンドに構築できるサービスである。利用者からのリクエストに応じて、仮想ネットワーク、ソフトウェア環境の配備をオンデマンドで構成することが可能で、2017年より試験運用、2018年より本運用を開始する予定である。

本ガイドラインはパブリックレビュー版です。
ご意見等は cld-office-support@nii.ac.jp までお送り下さい。



<http://cloud.gakunin.jp/>

学認クラウド

検索

文中に記載されている会社名、各製品名は、一般に各社の商標または登録商標です。

大学・研究機関のためのクラウドスタートアップガイド (パブリックレビューVer.1.0)

平成28年9月20日 発行

発行 大学共同利用機関法人 情報・システム研究機構
国立情報学研究所 学術基盤推進部 学術基盤課 クラウド支援室

〒101-8430 東京都千代田区一ツ橋2丁目1番2号

TEL 03-4212-2212 FAX 03-4212-2230

E-mail cld-office-support@nii.ac.jp
