情報システム調達ガイドライン

情報環境推進本部

1　情報システムの調達、導入、運用・管理にあたり、事前に、各部局等における責任者ならびに実効性のある体制を定めておくこと。本学に期待されている社会的責任に鑑み、委託想定先である専門業者等にすべてを任せきりにすることなく、不明な点については、事前に情報環境推進本部へ相談し、遺漏のないシステム調達とすること。

2　情報システム調達の最適化の実現を図るため、対象となる情報システムについては、契約担当部署への調達手続き依頼の、原則１ヶ月前までに CIO 補佐役に対して最適化確認の申請をすること。なお申請の内容によっては、システムの導入に大幅な修正が求められたり、情報システムの調達・構築そのものが許可されない場合があることに留意すること。(「情報システムの最適化実現に係る確認体制について」(https://www.oicte.hokudai.ac.jp/ict/optimisation.htm を参照)

3　情報資産の格付けに応じ、1. で定めた責任者および体制において、以下の例示を参考として、適切な情報の取り扱い、セキュリティ対策を予め定め、調達後、実際に実施すること。(情報資産の格付けについては、「国立大学法人北海道大学における情報資産の格付け及び取扱制限に関する内規」を参照のこと。)

3.1　最重要情報（機密性３＋）については、物理的、論理的に隔離された計算機、ストレージ、システム環境を用いることとし、インターネット等、担当部署からのみ接続可能な状態にすること。

3.2　機密性の高い情報（機密性３）を取り扱うシステムを構築する場合、多層・多重防御の考え方を取り入れ、一度の侵入や設定ミスで情報漏洩が生じないよう、十分配慮すること。(例えば、隔離した VLAN 内にシステムを構築し、さらに暗号化などの対策を講じる、部署内のみで使用するファイルでも必ずパスワード保護を行う、など)

3.3　物理的セキュリティ（サーバの設置場所の施錠や無停電電源、耐震・耐火対策などの環境条件や事業継続性の観点）にも十分配慮し、機密性に留意の上

で、本学の提供するクラウドサービスやハウジングサービスを利用すること。

3.4　学内設置のサーバ（情報基盤センターによるインタークラウドサーバの各種サーバや情報環境推進本部が運用する事務用の仮想サーバなどの、プライベートクラウドを含む）については、学外からのアクセスのため「インバウンド通信制限解除申請」による審査を受ける必要があるが、学外に設置されるサーバについても同レベル以上の対応が必要であり、必要最小限の通信ポート番号ならびに送信元（インターネット全体からの接続とならぬよう、範囲をできるだけ絞ることが望ましい）に限定すること。

4　オンプレミス（個別にハードウェアを学内に設置する形態）でのサーバの購入は可能な限り避け、本学（情報環境推進本部、情報基盤センター）がサーバやストレージを提供するプライベートクラウド、クラウド事業者が商用サービスとしてサーバやストレージなどを提供するパブリッククラウド、両者の組み合わせによるハイブリッドクラウドを、情報セキュリティポリシーや、必要となるシステムの条件に応じて選択し、利用するよう、努めること。

5　システムの構築にあたり必要となるサーバ環境について、1. で示した責任者や体制のもとで十分検討し、取り扱う情報資産の格付けに応じて適切なサービスを選択し、それぞれに応じたセキュリティ対策を講じることが必要である。
参考までに、本学において可能な選択肢として、以下が考えられる。なお、それぞれの選択肢において、サービス提供側で講じられているセキュリティ対策を確認し、不足している部分については、サービス提供側において、利用時に補う必要がある。

5.1　Web ホスティング（情報環境推進本部）

・部局や研究室などのホームページ公開向けのホスティングサービス
・WordPress＋StaticPress（CMS で編集し、静的サイトとして公開）
・提供条件：機密性 1 、完全性 1 、可用性 1

5.2　事務クラウド（情報環境推進本部）

・業務用のシステム構築に利用可能な仮想サーバを提供

5.3　事務ホスティング（情報環境推進本部）

・扱う情報について特段の制限はないが、格付けに応じたセキュリティ対策

をとる必要がある。事務ホスティング（情報環境推進本部）

・業務用の学内向けホスティングサービスを提供

・提供条件：機密性１～２、完全性１～２、可用性１

5.4　仮想プライベートクラウド（情報環境推進本部）

・業務用のシステム構築に利用可能な仮想サーバを提供

・学外設置のクラウドを利用するが、専用線で学内ネットワークと直結し、論理的に学内扱いとして利用可能。インターネット経由の学外接続については、インバウンド通信制限解除の申請を行うことで、本学の FW を経由して可能。

・提供条件：機密性１～３、完全性１～２、可用性１（学外へのネットワーク接続の遮断時、定期メンテナンス等において一時的に使用できなくなる可能性有り）

5.5　ハウジングサービス（情報基盤センター）

・情報基盤センターの施錠されたサーバルーム内に物理サーバを設置可能（場所貸しであり、設置する機器に関する管理は設置主体が全面的に担う必要がある）

5.6　研究クラウド（学際大規模計算機システム：情報基盤センター）

（https://www.hucc.hokudai.ac.jp/）

・研究プロジェクト向けのクラウドサービス

・仮想サーバ、物理サーバ、GPU サーバ、クラウドストレージを提供

・提供条件：機密性１～３（最重要情報（機密性３+）については取り扱い不可)、完全性１、可用性１

・リソースが逼迫しているため、JHPCN（学際大規模情報基盤共同利用・共同研究拠点）など情報基盤センターの計算資源を利用した公募研究課題へ応募、採択された場合を除き、新規での利用を受け付けていないことがある。

・クラウドストレージ（Dropbox のようなストレージとして、遠隔バックアップあり。情報基盤センター利用登録者 100GB まで無料）については、研究データの安全な保管を目的として提供している。

5.7　パブリッククラウド

・学外で一般に提供されている「仮想サーバ」などのパブリッククラウドを利用する際には、提供条件について、国立情報学研究所が提供する「学認ク

ラウド導入支援サービス」（https://cloud.gakunin.jp/cas/）のスタートアップガイド、チェックリストを活用し、導入目的やセキュリティ要件等に合致しているか事前に確認すること。
・パブリッククラウドを用いた調達にあたっては、本学における情報システム調達の最適化、ならびにシャドウ IT 化（本学のガバナンスが効かない状態での情報システム利用）を避けるため、必ず CIO 補佐役による確認を受けること。（特に、重要度、複雑度、技術的難易度が高いものと予想されるシステムや、継続性が懸念されるサービスについては、明らかに問題をはらむ内容の場合、利用を承認できないこともあることから、調達・発注に先んじて、検討段階から早めに情報環境推進本部に相談すること。）
・最重要情報（機密性３+）を扱うシステムは、パブリッククラウドで扱うことができない。それ以外の機密情報を扱う場合でも、その内容や程度に応じて、適切な対応を行う（仮想プライベートクラウドや仮想ネットワークにより分離する、秘密分散や高度な暗号化を施す、多層・多重防御を実装するなど）ことで利用できる可能性もあるが、必ず CIO 補佐役による確認を受けること。
・パブリッククラウドサービスで機密性３の情報を取り扱う場合は、原則として SaaS（Software as a Service: ソフトウェアやアプリケーションとしてクラウドサービスを利用する形態）に限定することとし、企画段階及び予算要求段階から、CIO 補佐役の関与の下（別紙様式による事前相談制）で、検討するものとする。なお、「政府情報システムのためのセキュリティ評価制度（ISMAP）」において登録されたサービスから調達することを原則とする。クラウドサービス（SaaS）が ISMAP に登録されていない場合、第三者による認証制度（ISO/IEC 27017、JASA クラウドセキュリティ推進協議会 CS ゴールドマーク、米国 FedRAMP）による認証を取得しているサービスから CIO 補佐役の承認を受け利用することができる。
・SaaS の場合、基本的にはサービス提供者側がその約款に従って情報セキュリティ上の責任を負うが、利用者側では約款に記載された条件を精査するとともに、利用者側でのサービスの不適切な設定及び不適切なデータの取り扱いによって生じる情報セキュリティ上の責任は利用者が負うことになるので、細心の注意をはらうこと。
・パブリッククラウドサービスに保存される利用者データの可用性の観点か

ら、日本の法律及び締結された条約が適用される国内データセンタと日本に裁判管轄権があるクラウドサービスを選択すること。ただし、データの保存性、災害対策等からバックアップ用のデータセンタが海外にあることが望ましい場合、又は争訟リスク等を踏まえ海外にあることが特に問題ないと認められる場合はこの限りではない。

・パブリッククラウドサービス利用時の伝送路は暗号化すること。格納されるデータやデータベースについても、機微な情報については暗号化を行うものとする。

6　システムの保守、運用・管理、セキュリティ対策については、1. で示した体制において責任を持って対応し、特に以下の点に留意すること。

調達後の運用に際し、システムに係る運用・管理責任者ならびに運用・管理体制を明確化すること。

6.1　本学担当者によるシステムの運用・管理が事実上難しい場合は、保守、運用・管理、セキュリティ対策の委託契約を行い、各部局等の責任者によるガバナンスの下、適切なシステムに係る運用・管理体制を担保すること。ただし、冒頭に記したとおり、委託想定先である専門業者等にすべてを任せきりにすることのないよう、十分な監督を行い、最低でも月次での報告や情報交換を行うことを要件とすること。また、委託契約の内容についても、疑義があれば速やかに情報環境推進本部に相談すること。

6.2　セキュリティパッチの適用など脆弱性への対応については、運用・管理責任者の責任のもと、速やかに実施する体制を整備すること。（可能な限り、自動アップデートを推奨する。）

6.3　システムへのアクセスログ、サーバのログは必ず取得、保存すること。保存期間としては、原則 18 ヶ月以上保存とし、そのための記憶領域も調達内容に含めること。

6.4　インシデント発生時には、速やかに情報環境推進本部情報セキュリティ対策室（HU-CSIRT）に報告するとともに、その後の対応についても協力すること。

別紙様式

パブリッククラウド（SaaS）で機密性３の情報を取り扱う場合の事前相談について

部局名
職　名
氏　名

１．利用したいパブリッククラウド名（SaaS）

２．上記で利用するサービス内容

３．利用対象者

４．サービスの種別（特定の業務か、コミュニケーション系か）等

５．他のサービスやシステムとの連携

６ 取り扱う情報

(1)　本学の情報セキュリティポリシー等に基づいた情報の格付け
（機密性、完全性、可用性）

（2）　機密性3の取り扱う情報（氏名、住所、メールアドレス等）

附則　令和５年５月改正