

答 申 第 4 号
令和2年8月20日

芦屋市教育委員会 様

芦屋市情報公開・個人情報保護審査会
会長 島 田 茂

クラウド型学習支援ソフトの導入に伴うオンライン結合について(答申)

令和2年7月30日付け芦教打第359号による下記の諮問について、以下のよう
に答申します。

記

第1 諮問内容

新型コロナウイルス感染拡大防止に伴い、小中学校が休校となったことを受け、オンライン学習の必要性が急速に高まり、新型コロナウイルス感染拡大の第2波、第3波や激甚化する災害における休校措置に備えることが急務となっている。令和元年度補正予算で示された国の施策でもある「GIGAスクール構想の実現」が前倒しされ、児童生徒一人一台PCの早期実現、オンライン学習を可能にするための家庭への支援、クラウド型学習支援ソフト（以下、「ソフト」という。）導入に係る工事などをすべて今年度中に実施することとなった。

また、本年度より実施された新学習指導要領では、新しい時代に必要となる資質・能力の向上を図るための指導及び「主体的・対話的で深い学び」の視点に立った授業改善を、ICTを有効に活用しつつ行うことが求められている。

そこで芦屋市教育委員会では、文部科学省通知「GIGAスクール構想の実現」及び「教育情報セキュリティポリシーに関するガイドライン（令和元年12月版）」に沿い、セキュリティを担保した上で、オンライン学習が可能なソフトの導入を考えている。今回の導入で参考としているソフトは、昨年度の諮問の際に参考としたソフトとは、別のものである。

ソフト導入に当たり、インターネット回線を利用し、児童生徒の学習情報等をソフト提供事業者（以下、「事業者」という。）と契約関係にあるクラウドサー

バに保管し、随時利用することになるため、芦屋市個人情報保護条例第15条第2号により、審査会に諮問されたものである。

第2 実施機関からの説明

審査会は、ソフトの導入に関して、芦屋市教育委員会（以下、「実施機関」という。）から説明を受け、以下の事項を確認した。

1 提供の目的

実施機関が事業者には、必要と認める情報の提供を行い、児童生徒の学習情報（学習活動における資料やノート、作品等）を電子データ化し、それらを事業者と契約関係にあるクラウドサーバに集約する。

このシステム構成を生かして新型コロナウイルス感染拡大や災害等に係る学力保障の一環として家庭でのオンライン学習を実施できるようにするとともに、児童生徒の学習意欲や学力の向上を図り、教員の授業改善に生かすことを目的とする。

2 実施機関が事業者へ提供する情報

- (1) 学校名
- (2) ユーザID
- (3) パスワード
- (4) 児童生徒・教職員氏名
- (5) 学年・クラス
- (6) 学習情報（成果物や授業記録、写真）

3 事業者が管理（保有）しクラウドサーバに保管する個人情報

- (1) 学校名
- (2) ユーザID
- (3) パスワード
- (4) 児童生徒・教職員氏名
- (5) 学年・クラス
- (6) 学習情報（成果物や授業記録、写真）

4 導入目的

- (1) 教育的効果

ア 新型コロナウイルス感染防止や災害等に係る休校措置等における学力保障

感染症対策や災害等で休校を余儀なくされた場合でも、児童生徒の学びを進められるよう、双方向のオンライン学習を整備し、児童生徒の学力を保障することが全国的な課題となっている。今年度中に懸念されている第2波、第3波を想定した上で、オンライン環境の構築を早急に行い、この環境を用いた学力保障が求められている。

また、グループワーク機能(協働作業・協働編集)を活用して、休校時においても、クラスの仲間と協働的な学びを実現することで、多様な考えや意見に触れお互いの思考を深めることができ、離れていても児童生徒がつながりを感じ心が安定すると考える。

イ 「学習の効率化」と「主体的・対話的で深い学び」の実現に向けた授業改善

今年度の教育課程において、例年に比べ授業時数が大きく下回ることが危惧されており、学習の効率化は喫緊の課題である。そこで実施機関では、基礎問題は家庭学習で行い、発展問題や学習についての協議から始める「反転学習」の導入を考えている。「反転学習」の良さは、学習の効率化はもちろんのこと、学習の主体性や協働による深い学びにつながる学習展開が可能となるところにある。さらに、この「反転学習」には、学習支援ソフトが不可欠で、児童生徒が学習課題について発表ノートに記述したものを教員が事前に回収し、次の授業前に把握することで、ポイントを絞った指導が可能となり、学習の効率化に大きく寄与する。また、教員への質問が場所や時間(教員の就業時間は守った上で)を超えて可能となることで、子どもの学習意欲の向上も見込める。

また、今年度だけでなく、継続的に上記のような学び方を実施することは、児童生徒の学力の向上や教員における授業改善の実現に大きく寄与すると考えている。

(2) 校務の効率化

ア 教員同士の情報共有

ソフトを教員同士の事務連絡やお知らせなど情報共有のために活用することで、職員朝礼等の簡素化を図り、教員の働き方改革に寄与する。

イ 家庭や児童生徒への連絡として

電子連絡板機能を活用して家庭や児童生徒に連絡することが可能となり、休校下における急な連絡事項やお知らせなどを即時に伝えることができ、業務の効率化が図られる。

5 個人情報の保護措置について

(1) ソフトの利用における芦屋市の個人情報の利用範囲

ソフトの利用における「個人情報」とは、芦屋市個人情報保護条例第2条第2号に定められているものとする。

事業者は、ソフトを提供するために必要な範囲においてのみ個人情報を収集し、又は利用することができ、事業者の営業等の目的で利用してはならない。ソフトを提供するために必要な範囲とは、次のアからオまでに掲げる利用とし、実施機関に対して利用したことを報告することとする。

ア ソフトの安全を保ち円滑に利用できるようにするため。

イ ソフトの不正利用防止のため。

ウ ソフトの維持、メンテナンス、不具合対応のため。

エ ソフトに関する芦屋市からの問い合わせ、要望等の対応のため。

オ その他、アからエまでに付随する目的のため。

(2) 実施機関が講じる個人情報の保護措置

ア 実施機関は、個人情報の取扱いについて学校で定期的に研修を実施する。

イ 実施機関は、ソフトにログインできる端末を実施機関が貸与したものに限定した上で、ID及びパスワードを厳重に管理し、データの流出や持ち出しが発生しないよう徹底する。

ウ ソフトで使用する児童生徒のID管理は、管理者権限により制限設定を行うことで、実施機関と事業者以外は変更等ができないようにする。

エ クラウドサーバへの接続は、安全性の高いSSL暗号化通信を用いる。

オ 実施機関は、事業者がクラウドサーバに保存された個人情報を適切に管理しているか、また本来の目的以外の目的で利用していないか定期的に確認する。

(3) 実施機関が事業者を求める個人情報の保護措置

ア 事業者は、個人情報の取扱いについて事業者内で定期的に研修を実施すること。

イ 事業者は、クラウドサーバにログインするためのID及びパスワードによるアクセス権限を設定、厳重に管理し、利用可能な者を必要最小限とすること。

ウ 事業者は、クラウドサーバのデータセンターを日本国内に設置し、紛争に関する準拠法を日本法とし、管轄裁判所を日本とすること。

エ 事業者は、実施機関が提供する個人情報を含むデータについて、実施機関

- が卒業生等の児童生徒のデータを適宜消去できる仕様とすること。なお、事業者は、バックアップデータについて、30日間保存後、消去すること。
- オ 事業者は、「教育情報システムのクラウドサービス利用に係る要領」（別紙1）を遵守しなければならない。
- カ 事業者は、事業者及びクラウドサーバを提供する事業者の責めに帰する理由により、実施機関に損害を与えた場合は、その損害を賠償しなければならない。
- キ 実施機関は、事業者と覚書（別紙2）を締結し、個人情報の取扱い等について規定する。事業者と直接契約をしない場合は、契約の相手方及び事業者と三者で覚書を締結する。

第3 審査会の判断

本諮問は、令和元年度答申第2号において本審査会が4つの問題点を指摘し、オンライン結合により児童生徒の学習情報を取り扱うことは適当ではないと判断したソフトの導入について、問題点を改めたうえで再度諮問されたものである。

問題点は、以下のとおりである。

- 1 実施機関が前回の諮問において参考とした事業者のプライバシーポリシーでは、実施機関の同意なしに当該ソフト導入の本来の目的である学習支援以外にも収集された個人情報が利用されることが前提となっている。
- 2 事業者がクラウドサーバに保存された個人情報を本来の目的以外に利用することについて、実施機関の意見が適正に反映されているかどうか、また、実施機関の知らないところで目的外利用がなされていないかをチェックする仕組みが必要となるが、それらの仕組みの内容が具体的に示されていない。
- 3 事業者のプライバシーポリシーでは、個人を特定することができない形式のデータを収集し、これを統計情報として利用することがあるとしているが、事業者が適切に統計データを収集・利用していることを実施機関が確認する方法が示されていない。
- 4 ソフトの導入においては、実施機関と直接契約関係にない事業者等が学習情報等を適切に管理しているか、確認する方法が示されていない。

以上の問題点について検討すると、1については、本諮問において参考としている事業者のプライバシーポリシーには、ソフトの提供に必要な範囲におい

でのみ個人情報を収集し、利用することができることが明確に規定されている。また、当該ソフトの調達仕様書においても同様に個人情報の収集及び利用の範囲が規定されているため、仮に参考としたソフト以外のソフトが導入されたとしても個人情報の収集及び利用が適切に行われることが確認できる。

2及び3についても、調達仕様書及び事業者のプライバシーポリシーにおいて、収集した個人情報を学習支援の目的以外に利用できないことが明記されており、また本来の目的で利用した場合においても実施機関に報告することとされているため、事業者が個人情報を実施機関の知らないところで目的外利用又は統計情報として利用することはないことが確認できる。

4については、実施機関が代理店を通して契約する場合は、事業者、代理店及び実施機関の三者で覚書を交わし、個人情報の適正な管理を促すとして覚書の案（別紙2）を示している。

本審査会は、4つの問題点以外にも情報セキュリティポリシーにクラウドサービスの利用に関する規定が置かれていないことを指摘したが、実施機関は、新たに教育委員会のセキュリティポリシーとして「芦屋市教育情報ネットワークシステム対策基準」の案を示し、さらにクラウドサービスの利用に関しては、「教育情報セキュリティポリシーに関するガイドライン」に準じて「教育情報システムのクラウドサービス利用に係る要領」の案（別紙1）も示している。

また、実施機関は、児童生徒の保護者にソフトの利用について周知する予定であることも説明している。

以上のことから本審査会は、実施機関の説明の通りに適切にソフトが運用されるのであれば、本諮問におけるオンライン結合により、児童生徒の権利利益が侵害されるおそれはなく、ソフトの導入は、適当であると判断する。

なお、諮問の時点では、案であった「芦屋市教育情報ネットワークシステム対策基準」、「教育情報システムのクラウドサービス利用に係る要領」及び覚書の施行文を後日審査会に提出することを求める。

以 上

審査会の経過

年 月 日	処 理 内 容
令和2年7月30日	諮問書の受理
令和2年7月30日	第1回審議
令和2年8月20日	第2回審議

芦屋市情報公開・個人情報保護審査会委員

氏 名	役 職 名	備 考
島田 茂	甲南大学名誉教授	会 長
大月 一弘	神戸大学大学院国際文化学研究科教授	職務代理
伊藤 明子	弁護士	
岩本 洋子	弁護士	
大久保 規子	大阪大学大学院法学研究科教授	
亀若 浩幸	弁護士	

教育情報システムのクラウドサービス利用に係る要領(案)

(目的)

第1条 この要領は、芦屋市学校園ネットワークにおける教育情報システムのクラウドサービス利用を安全に行うため、クラウド事業者が実施する情報セキュリティ対策及びクラウドサービス提供ポリシーに係る確認等、必要な事項を定め、教育情報セキュリティの確保を図ることを目的とする。

(定義)

第2条 この要領で使用する用語の意義は、特段の定めがある場合を除くほか、「芦屋市情報セキュリティ基本方針に関する要綱」及び「文部科学省教育情報セキュリティポリシーガイドライン（令和元年12月版）」で使用する用語の例による。

2 この要領において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1)クラウド事業者

自らのサービスのセキュリティに加え、IaaS/PaaS事業者によるインフラ基盤やプラットフォーム基盤のセキュリティを確認し、クラウドサービスを提供しているSaaS事業者。主に、学習支援ソフトウェア事業者。

(2)クラウド利用者

クラウドサービスの選定・契約の主体となり得る者。主に教育委員会。

(3)エンドユーザ

教職員や児童生徒。

(利用者認証)

第3条 クラウド利用者は、クラウド事業者における当該クラウドサービスを提供する情報システムの運用もしくは開発に従事する者又は管理者権限を有する者について、適切な利用者確認がなされていることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意サービス提供定款や契約書面上で確認または合意しなければならない。



2 クラウド利用者は、当該クラウドサービスのログインに関わる認証機能の提供をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

3 クラウド利用者側管理者権限を有する者のID管理について、当該各号を遵守しなければならない。



(1) 教育情報システム管理者は、管理者権限等の特権を付与されたIDを利用

する者を必要最小限にし、当該IDのパスワードの漏えい等が発生しないよう、当該ID及びパスワードを厳重に管理しなければならない。

- (2) 教育情報システム管理者は、特権を付与されたID及びパスワードの変更について、外部委託事業者に行わせてはならない。
- (3) 教育情報システム管理者は、特権を付与されたID及びパスワードについて、教職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。
- (4) CEISO及び情報システム管理者は、特権を付与されたIDを初期設定以外のものに変更しなければならない。

(アクセス制限)

第4条 クラウド利用者は、当該クラウドサービスに対して、アクセスする権限のない者がアクセスできないように、システム上制限する機能の提供をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。



- 2 クラウド利用者は、クラウド事業者の提供するアクセス制御機能を用いて、情報資産毎に、許可されたエンドユーザのみがアクセスできる環境を設定しなければならない。

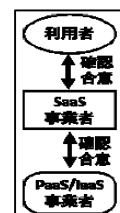
(クラウドに保管するデータの暗号化)

第5条 クラウド利用者は、当該クラウドサービスへのデータの保管に際し、情報漏えい等に備えて、暗号化等の保護措置を講じられていることを、クラウド事業者にサービス提供定款や契約書面上で確認または合意しなければならない。



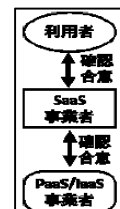
(マルチテナント環境におけるテナント間の安全な管理)

第6条 クラウド利用者は、複数のクラウド利用者がクラウドリソースを共用する環境において、特定のクラウド利用者に対して発生したセキュリティ侵害が、他のクラウド利用者に影響を与えないように対策が講じられていることを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。



(クラウドサービスを提供する情報システムに対する外部から悪意のある脅威の侵入を想定した技術的セキュリティ対策)

第7条 クラウド利用者は、当該クラウドサービスを提供する情報システムを監視し、セキュリティ侵害を検知することを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

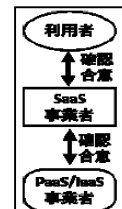


- 2 クラウド利用者は、当該クラウドサービスを提供する情報システムのインターネット接続境界において、クラウド利用者以外による不正な通信・侵入を

防ぐ措置を講じるとともに、外部脅威の侵入を検知し、防御する対策を講ずることを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

(情報の通信経路のセキュリティ確保)

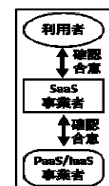
第 8 条 クラウド利用者は、教育情報システムのインターネット境界から当該クラウドサービスを提供する情報システムまでの情報の通信経路において、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準・手順等の整備、通信の暗号化等）をクラウド事業者に求め、合意のうえ、利用しなければならない。



2 クラウド利用者は、クラウド事業者が保守運用等を遠隔で行う場合の、保守運用拠点と管理区域間での通信回線及び通信回線装置の管理について、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準・手順等の整備、通信の暗号化等）をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

(クラウドサービスを提供する情報システムの物理的セキュリティ対策)

第 9 条 クラウド利用者は、当該クラウドサービスのサーバ等の管理条件を当該各号の対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。



(1) 機器の取付け

サーバ等の機器の取付けを行う場合は、地震、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置及び容易に移動されない場所に設置しなければならない。

(2) サーバの冗長化

サーバ等のハードディスクを冗長化しなければならない。

(3) 機器の電源

ア サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

イ 落雷等による過電流に対して、必要に応じて、サーバ等の機器を保護するための措置を講じなければならない。

(4) 通信ケーブル等の配線

ア 通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

イ クラウド事業者や契約により操作を認められた外部委託事業者以外の

者が配線を変更，追加できないように必要な措置を施さなければならない。

(5) 機器の定期保守

サーバ等の機器の定期保守を実施しなければならない。

(6) 機器の廃棄等

機器を廃棄する又はリースを返却する場合は，機器内部の記憶装置から，すべての情報を消去の上，復元不可能な状態にする措置を講じなければならない。

2 クラウド利用者は，クラウド事業者側の管理区域（サーバ等を設置）及び保守運用拠点の管理において，当該各号の対策をクラウド事業者に求め，サービス提供定款や契約書面上で確認または合意しなければならない。

(1) 管理区域の構造等

ア 管理区域とは，ネットワークの基幹機器及び重要な情報システムを設置し，当該機器等の管理及び運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

イ 管理区域を設置及び管理する管理者（以下「管理区域の管理者」という。）は，管理区域を可能な限り地階又は1階に設けてはならない。

ウ 管理区域の管理者は，管理区域から外部に通ずるドアは必要最小限とし，鍵，監視機能，警報装置等により，許可されていない者の立入りを防止しなければならない。

エ 管理区域の管理者は，情報システム室内の機器等に，必要に応じて，転倒及び落下防止等の耐震対策，防火措置，防水措置等を講じなければならない。

オ 管理区域の管理者は，可能な限り管理区域を囲む外壁等の開口部をすべて塞がなければならない。

カ 管理区域の管理者は，管理区域に配置する消火薬剤や消防用設備等が，機器等及び記録媒体に影響を与えないようにしなければならない。

(2) 管理区域の入退室管理等

ア 管理区域の管理者は，管理区域への入退室を許可された者及び目的のみに制限し，入退室管理簿の起債による入退室管理を行わなければならない。また，必要に応じてICカード，指紋認証等の生体認証を併せて行わなければならない。

イ 管理区域に入室する場合は，身分証明書等を携帯させ，必要に応じ，提示を求めなければならない。

ウ 管理区域の管理者は，外部からの訪問者が管理区域に入る場合は，必要に応じて立ち入り区域を制限した上で，管理区域への入退室を許可さ

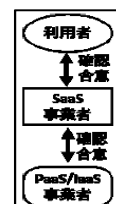
れた職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

(3) 機器等の搬入出

搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は機器等の搬入出を委託した業者に確認を行わせなければならない。

(クラウドサービスを提供する情報システムの運用管理)

第10条 クラウド利用者は、クラウド事業者に対して、サービスの一時停止等クラウド利用者に影響があり得る運用手順の有無、有る場合にはクラウド利用者への影響範囲（時間、サービス内容）、連絡方法等について情報提供を求め、クラウド利用者が業務運営に支障がないことを確認し、合意しなければならない。



2 クラウド利用者は、当該クラウドサービスにおけるサーバ等のハードディスクを冗長化するようクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

3 クラウド利用者は、当該クラウドサービスにおけるデータバックアップについて、ファイルサーバ等に記録された情報はサーバの冗長化対策に関わらず、必要に応じてバックアップを実施するものごとをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

4 クラウド利用者は、当該クラウドサービスにおける情報セキュリティの確保や監査に必要なログの取得について、当該各号に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

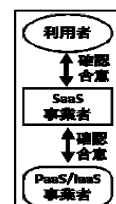
(1) 各種ログ及び情報セキュリティの確保に必要な記録を必要に応じて、取得し、一定の期間保存しなければならない。

(2) ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

(3) 取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

(クラウドサービスを提供する情報システムのマルウェア対策)

第11条 クラウド利用者は、クラウドサービスを提供する情報システムを構成するサーバ及び運用管理端末等について、マルウェア対策を講じることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。



2 クラウド利用者は、内部システムに侵入した攻撃を検知して対処するために、

通信をチェックする等の対策を講じることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

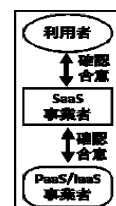
(クラウド利用者側のセキュリティ確保)



第12条 クラウド利用者は、クラウドサービスにアクセスする利用者側端末について、保管するデータの外部流出、改ざん等から保護するために必要な措置を講じなければならない。

2 クラウド利用者は、標的型攻撃による外部からの脅威の侵入を防止するために、エンドユーザへの教育や入口対策を講じなければならない。

(クラウド事業者従業員の人的セキュリティ対策)



第13条 クラウド利用者は、クラウドサービスに関わるクラウド事業者従業員に対して、クラウド事業者の情報セキュリティポリシー及び保守運用管理規程等を遵守することをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

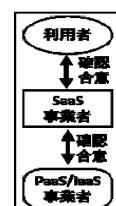
2 クラウド利用者は、クラウドサービスに関わるクラウド事業者従業員に対して、業務に用いるID及びパスワードその他の個人認証に必要な情報及び媒体について、部外者及び業務に関わらない従業員に漏えいすることがないように、適切に管理することをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

3 クラウド利用者は、クラウドサービスに関わらない従業員等がクラウド利用者のデータを知り得る状態にならないよう、業務に関わるクラウド事業者従業員に対して秘匿を義務づけることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

4 クラウド利用者は、クラウド利用者のデータ及びデータを格納した端末機器又は電磁的記録媒体の外部持ち出しについて、クラウド利用者の許可なく外部持ち出しできないこと及び外部持ち出しにおける安全管理手順をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

5 クラウド利用者は、クラウドサービスを提供する情報システムを構成するサーバ及び運用管理端末等に、マルウェアを侵入させないように、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

(データの廃棄等について)



第14条 クラウド利用者は、サービス利用終了時等において、クラウド利用者のデータが不用意に残置されないよう、適切に破棄するための流れについてサービス提供定款や契約書面上で確認または合意

しておかなければならない。

- 2 クラウド利用者は、サービス利用終了時等におけるデータの扱いについて、スムーズに回収、次期システムへの移行等を行えるよう、その措置の流れについてサービス提供定款や契約書面上で確認または合意しておかなければならない。

(守秘義務、目的外利用及び第三者への提供の禁止)

- 第15条 クラウド利用者は、クラウド事業者と契約時に守秘義務、目的外利用及び第三者への提供の禁止条項を締結しなければならない。クラウドサービス事業者がコンテンツにアクセスできるかどうかを確認し、サービスに係る情報及び受託した情報に関する守秘義務、目的外利用及び第三者への提供の禁止条項について、サービス提供に係る契約に含めなければならない。契約には、当該条項に違反したクラウドサービス事業者に対する損害賠償規定を含める。



(準拠する法令、情報セキュリティポリシー等の確認)

- 第16条 クラウド利用者は、クラウド事業者がどのような規範に基づいてサービス提供するか開示を求め、クラウド利用者の準拠する法令、情報セキュリティポリシーを確認し、それらとの整合を確認しなければならない。(クラウド事業者の準拠する認証制度、個人情報保護指針、プライバシーポリシー、情報セキュリティに関する基本方針及び対策基準、保守運用管理規程等)



(クラウド事業者の管理体制)

- 第17条 クラウド利用者は、クラウド事業者に対して、教育情報セキュリティポリシー等の遵守を担保する管理体制が整備されているか、クラウド事業者の組織体制を確認し、合意しなければならない。

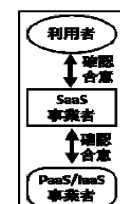


- 2 次の各号に、確認すべき項目を示す。

- (1) サービスの提供についての管理責任を有する責任者の設置
- (2) 情報システムについての管理責任を負い、これについて十分な技術的能力及び経験を有する責任者(システム管理者)の設置
- (3) サービスの提供に係る情報システムの運用に関する事務を統括する責任者の設置

(クラウド事業者従業員への教育)

- 第18条 クラウド利用者は、クラウド事業者に、従業員に対して個人情報保護等の関係法令、守秘義務等、業務遂行に必要な知識、意識向上のための適切な教育及び訓練を実施し、十分な知識とセキュリティ意識を醸成することを求めなければならない。

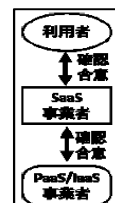


- 2 クラウド利用者は、クラウド事業者に、従業員への上記育成計画、教育実績

等の情報を提示させ、自らデータを管理する場合と同様の教育・訓練を実施しているかを確認しなければならない。

(情報セキュリティに関する役割の範囲、責任分界点)

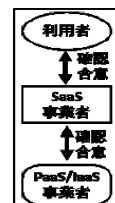
第19条 クラウド利用者は、クラウド事業者の情報セキュリティに関する役割の範囲と責任分界点について開示するよう求めなければならない。



2 クラウド利用者は、クラウド事業者の情報セキュリティに関する役割の範囲と責任分界点がクラウド利用者側で講ずる情報セキュリティ対策の役割の範囲と整合することを確認し、合意しなければならない。

(監査)

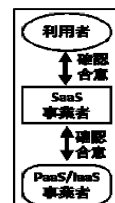
第20条 クラウド利用者は、クラウドサービスの監査状況、範囲・条件、内容等についてクラウド事業者が開示するよう求めなければならない。



2 クラウド利用者は、クラウド事業者によるクラウドサービスに関する監査レポート等を根拠にして、自らの関係法令、情報セキュリティポリシーと照らし合わせ、安全性が確保されているかについて確認しなければならない。

(情報インシデント管理及び対応フローの合意)

第21条 クラウド利用者は、情報セキュリティインシデント管理に関する責任範囲及びインシデント対応フローを、サービス仕様の一部として定めることについて、クラウド事業者に対して求めなければならない。



2 クラウド利用者は情報セキュリティインシデント管理に関する責任範囲及びインシデント対応フローを検証しなければならない。

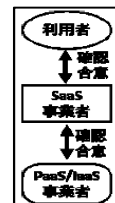
(クラウドサービスの提供水準及び品質保証)

第22条 クラウド利用者は、クラウドサービスの提供水準（サービス内容、提供範囲等）と品質保証（サービス稼働率、故障等の復旧時間等）を確認するとともに、それらの水準・品質が、業務遂行に求められる要求水準を満たすことを確認し、合意しなければならない。



(クラウド事業者の再委託先等との合意事項)

第23条 クラウド利用者は、クラウド事業者と合意したサービス履行内容及び情報セキュリティ対策について、クラウド事業者自らが実施する内容と、再委託先等に委託する内容も含めて提示することをクラウド事業者に求めなければならない。また、サプライチェーンリスク対策が適切に講じられていることをクラウド事業者に求めなければならない。



2 クラウド利用者は、1項の提示内容が、クラウド事業者と合意したサービス履行内容及び情報セキュリティ対策と整合していることを確認しなければならない。

(クラウド事業者のプライバシー保護に関する合意事項)

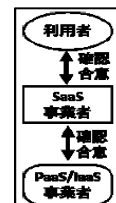
第 24 条 クラウド利用者の目的に必要な情報、またはエンドユーザの許可した情報を超えて個人情報の収集、維持、使用、共有をしないこと。

- 2 クラウドサービスの導入によって知り得た個人情報について、売買も含め、無断提供をしないこと。
- 3 クラウド利用者の目的を達成すること以外に、個人情報についてエンドユーザに対する行動ターゲティング広告をはじめとする、広告活動その他無断使用をしないこと。
- 4 クラウド利用者の目的を達成するため、またはエンドユーザによって許可された場合を除き、不必要な個人プロフィールを作成しないこと
- 5 クラウドサービスの運用等において、クラウド利用者に対する明確な通知・相談等の対応もなく、プライバシーポリシーに重大な影響を与えるような変更を行わないこと。
- 6 クラウド利用者と合意したサービス提供期間を超えて個人を特定する情報を保持しないこと。
- 7 個人情報を収集、使用、共有、および保持するのは、クラウド利用者によって承認された目的に限ること。
- 8 個人情報の取扱いについて、契約またはプライバシーポリシーで明確に示すこと。
- 9 個人情報の登録、変更、削除に関するサービスをクラウド利用者に提供すること。
- 10 個人情報に対する不正アクセス又は個人情報の紛失、破壊、改ざん、漏洩、盗難等のリスクに対し、適切な安全対策を講じること。また、個人情報を正確かつ最新の状態で管理すること。
- 11 サービス提供の全部又は一部を第三者に再委託又は代行実施させる場合には、個人情報保護法制等を遵守し、当該再委託先又は代行実施先について、同等の義務を課し、管理するものとする。
- 12 合併または他社による買収を伴う場合、後継企業が以前に収集した個人情報について同様の義務を負うことを条件に、個人情報を継続して管理するものとする。

(その他留意事項)

第25条 クラウド利用者は、クラウド事業者がサービスを安定して提供可能な企業・団体であるかについて考慮しなければならない。

2 クラウド利用者は、クラウド事業者間でのデータ形成の互換性が必ずしも保証されている訳ではないことから、事業者を変更する際のデータ移行の方法などについて、クラウド事業者にサービス提供定款や契約書面上で確認または合意しなければならない。



3 クラウド利用者は、クラウド事業者に対して、クラウドサービスにおいて扱う情報資産や情報システム等について、日本の法令が適用されること及び係争等における管轄裁判所が日本国内であることを確認すること。

附 則

この要領は、令和2年 月 日から施行する。

〇〇のクラウドサービス利用に関する覚書

芦屋市（以下「発注者」という。）、〇〇（以下「受注者」という。）及び〇〇（以下「クラウドサービス提供者」という。）は、発注者と受注者が令和〇年〇月〇日付けで契約を締結した「●●●」において、クラウドサービス提供者が提供するクラウドサービス「〇〇」（以下「本件サービス」という。）に関して次のとおり覚書を締結する。

（覚書の目的）

第1条 この覚書は、発注者が、授業支援ソフトとして本件サービスを利用するに当たり、受注者及びクラウドサービス提供者が遵守すべき事項を規定することを目的とする。

（サービス内容等）

第2条 クラウドサービス提供者が提供する本件サービスのサービス内容、機能、クラウドサービス基盤、プライバシーポリシー及びセキュリティ対策等については、別紙仕様書及び教育情報セキュリティポリシーに定めるとおりとする。

（文書の提出）

第3条 発注者から本件サービスに関する資料等の文書の提出を求められたときは、受注者及びクラウドサービス提供者は、速やかにこれを提出しなければならない。

（調査等）

第4条 発注者は、必要があると認めるときは、受注者及びクラウドサービス提供者に対して、本件サービスの提供状況等について、随時に調査し、又は報告を求めることができる。ただし、当該調査は、事前に調査対象となる受注者又はクラウドサービス提供者（以下、「調査対象者」という）に連絡し、当事者間で協議した上で、調査対象者の営業時間内において、調査対象者の事業の妨げにならないような方法で行うものとする。

（秘密の保持及び個人情報の保護）

第5条 受注者及びクラウドサービス提供者は、本件サービスの提供において知り得た事項を他に漏らし、又は他の目的に利用してはならない。

2 受注者及びクラウドサービス提供者は、秘密の保持並びに個人情報の保護に関して規程を制定し、それぞれの業務従事者に対し、その内容の教育指導等を行い、これを遵守させなければならない。

3 前2項に規定する義務は、この覚書に係る業務が終了し、又は契約が解除された後においても存続するものとする。

（目的外収集・利用の禁止）

第6条 受注者及びクラウドサービス提供者は、本件サービスを提供するために必要な範囲においてのみ個人情報を収集し、又は利用することができ、発注者及びクラウドサービス提供者の営業等の目的で利用してはならない。クラウドサービスを提供するために必要な範囲とは、次のアからオまでに掲げる利用とし、実施機関に対して利用したことを報告することとする。

ア クラウドサービスの安全を保ち円滑に利用できるようにするため。

イ クラウドサービスの不正利用防止のため。

ウ クラウドサービスの維持，メンテナンス，不具合対応のため。

エ クラウドサービスに関する芦屋市からの問い合わせ，要望等の対応のため。

オ その他，アからエまでに付随する目的のため。

（第三者への提供の禁止）

第7条 受注者及びクラウドサービス提供者は，本件サービスを提供するために収集し，又は作成した個人情報記録された資料等を，発注者の承諾なしに第三者に提供してはならない。

（複写，複製の禁止）

第8条 受注者及びクラウドサービス提供者は，本件サービスを提供するために発注者から提供を受けた個人情報記録された資料等を，発注者の承諾なしに複写し，又は複製してはならない。

（適正管理）

第9条 受注者及びクラウドサービス提供者は，本件サービスを提供するために発注者から提供を受けた個人情報及び自らが収集した個人情報の漏えい，滅失又はき損の防止に努め，これらの個人情報を適正に管理しなければならない。また，これらの個人情報の管理及び発注者との連絡や確認を行うための管理責任者を定め，書面をもって発注者に通知するものとする。

（委託等の承認手続）

第10条 クラウドサービス提供者が本件サービスに関する業務を他に委託等する場合は，業務の開始日の10日前までに，委託等を行わせる相手方及び処理させる内容並びに本覚書で発注者が受注者及びクラウドサービス提供者に義務付けている内容を委託先等にも義務付ける旨を明記した承認申請書を発注者に提出し，発注者の承諾書を得なければならない。また，再委託等の処理が完了したときには，委託等の完了報告書を提出するものとする。

（クラウドサーバー等の管理）

第11条 クラウドサービス提供者は，クラウドサービス基盤を【 】
（以下「データセンター事業者」という。）と契約し，当該事業者が提供するクラウドサービスのサーバー等のデータセンターを利用する。受注者及びクラウドサービス提供者は，別紙「教育情報システムのクラウドサービス利用に係る要領」に規定するクラウドサーバーの利用に関する事項を満たしていることを，データセンター事業者に確認しなければならない。

2 受注者及びクラウドサービス提供者は，データセンター事業者を前項の事業者から変更する場合は，事前に発注者に知らせなければならない。

（持ち出しの禁止）

第12条 受注者及びクラウドサービス提供者は，本件サービスを利用するために発注者がデータセンターに登録した個人情報を，発注者の承諾なしに持ち出してはならない。また，発注者の承諾を得て当該個人情報を持ち出す場合には，個人の特性を不可能とするマスキング処理又は暗号化等，発注者の承諾を得た対策を講じなければならない。

(事故の場合の措置)

第13条 受注者及びクラウドサービス提供者は、この覚書に違反する事態が生じ、又は生ずるおそれがあることを知ったときは、速やかに発注者に報告し、発注者の指示に従うものとする。

(個人情報の消去等)

第14条 受注者及びクラウドサービス提供者が本件サービスを提供するために、発注者から提供を受け、又は受注者及びクラウドサービス提供者自らが収集した個人情報は、契約終了後直ちに消去するものとする。ただし、発注者が別に指示したときは当該方法によるものとする。

(損害賠償)

第15条 受注者及びクラウドサービス提供者は、故意又は過失により個人情報を漏えいしたとき、又はデータセンター事業者の責めに帰する理由により発注者又は第三者に損害を与えたときは、その損害を賠償しなければならない。

(専属的合意管轄裁判所)

第16条 この覚書に係る訴訟等については、発注者の事務所の所在地を管轄する裁判所を第一審の専属的合意管轄裁判所とする。

(協議)

第17条 この覚書に定めのない事項及びこの覚書に疑義が生じたときは、発注者、受注者及びクラウドサービス提供者が協議して定めるものとする。

本覚書締結の証として本書を3通作成し、発注者、受注者及びクラウドサービス提供者が記名押印の上、各自その1通を保有するものとする。

令和 年 月 日

発注者 芦屋市精道町7番6号
芦屋市
芦屋市長 伊藤 舞

受注者 ○○県(府)○○市○番○号
株式会社○○
○○長 ○○ ○○

クラウドサービス提供者
○○県(府)○○市○番○号
株式会社○○
○○長 ○○ ○○