神戸市情報システムのクラウドサービスの利用に係る基本方針

令和２年３月 16 日
情報セキュリティ統括責任者決定

神戸市情報セキュリティ対策基準 10.1.1 イの規定により、機密性２以上の情報についてクラウドサービスを利用する場合におけるセキュリティレベルの確保等にかかる基本方針を以下のとおり定める。

１　目的・趣旨

業務及び情報システムの高度化・効率化等の理由から、地方公共団体においても今後クラウドサービスの利用の拡大が見込まれる。なおクラウドサービスの利用に当たっては、クラウド基盤部分を含む情報の流通経路全般を俯瞰し、総合的に対策を設計（構成）した上で、セキュリティを確保する必要がある。

クラウドサービスを利用する際、市がクラウドサービスの委託先に取扱いを委ねる情報は、当該委託先において適正に取り扱われなければならないが、クラウドサービスの利用においては、適正な取扱いが行われていることを直接確認することが一般に容易ではない。

また、クラウドサービスでは、複数利用者が共通のクラウド基盤を利用することから、自身を含む他の利用者にも関係する情報の開示を受けることが困難である。クラウドサービスの委託先を適正に選択するためには、このようなクラウドサービスの特性を理解し、市による委託先へのガバナンスの有効性や利用の際のセキュリティ確保のために必要な事項を十分考慮することが求められる。

2　クラウドサービスの利用に係る遵守事項

○ 神戸市セキュリティ対策基準 10.1.1 イ

クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

○ 物理的・技術的セキュリティ管理基準（以下「管理基準」という。）6.2

クラウドサービスの利用にあたり、情報管理者は次の事項を遵守しなければならない。

ア　クラウドサービスで取り扱われる情報の格付及び取扱制限を踏まえ、情報の取り扱いを委ねることの可否を判断すること。

イ　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。

ウ　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。

エ　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。

オ　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。

＜遵守事項の逐条解説＞

(1)（管理基準 6.2 ア）

クラウドサービス（民間事業者が提供するサービスに限らず、クラウド基盤を利用して市が自らサービスを提供するものを含む。以下同じ。）で取り扱われる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。

※「情報の取扱いを委ねることの可否」についての考え方

クラウドサービスの利用に当たっては、情報の管理や処理をクラウドサービス事業者に委ねるため、その情報の適正な取扱いの確認が容易ではなくなる。そこで、適切なクラウドサービス事業者を選定することにより以下のようなリスクを低減することが考えられる。

・ クラウドサービスは、そのサービス提供の仕組みの詳細を利用者が知ることがなくても手軽に利用できる反面、クラウドサービス事業者の運用詳細は公開されないために利用者にブラックボックスとなっている部分があり、利用者の情報セキュリティ対策の運用において必要な情報の入手が困難である。

・ オンプレミスとクラウドサービスの併用やクラウドサービスと他のクラウドサービスの併用等、多様な利用形態があるため、利用者とクラウドサービス事業者との間の責任分界点やサービスレベルの合意が容易ではない。
・ クラウドサービス事業者が所有する資源の一部を利用者が共有し、その上に個々の利用者が管理する情報システムが構築されるなど、不特定多数の利用者の情報やプログラムを一つのクラウド基盤で共有することとなるため、情報が漏えいするリスクが存在する。
・ クラウドサービスで提供される情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用されることによるカントリーリスクが存在する。
・ サーバ装置等機器の整備環境がクラウドサービス事業者の都合で急変する場合、サプライチェーンリスクへの対策の確認が容易でない。

(2)（管理基準 6.2 イ）

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。

※「国内法以外の法令が適用されるリスク」についての考え方

国内法以外の法令が適用されるリスクとして、データセンターが設置されている国が、法制度や実施体制が十分でない、法の執行が不透明である、権力が独裁的である、国際的な取り決めを遵守しないなどのリスクの高い国である場合、データセンター内のデータが外国の法執行機関の命令により強制的に開示される、データセンターの他の利用者等が原因でサーバ装置等の機器が市のデータを含んだまま没収されるなどが考えられる。

※「委託事業の実施場所」についての考え方

バックアップデータ、サーバ装置内のデータ等、市の情報が存在し得る場所すべてを委託事業の実施場所として考慮することが必要である。

(3)（管理基準 6.2 ウ）

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。

（留意事項）

情報管理者は、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。

・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

・取り扱う情報の可用性区分の格付に応じた、サービス終了または変更の際の事前告知の方法・期限及びデータ移行方法

※「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」についての考え方

クラウドサービス事業者が、何らかの理由でクラウドサービスの継続的な提供ができなくなった場合に、他のクラウドサービス事業者に対し、情報の移行を円滑に実施することにより、利用者側での業務を継続できるようにすることが求められる。

そのため、移植性又は相互運用性を確保する観点から、可能な限り、標準化されたデータ形式やインタフェースを使用することが望ましい。

(4)（管理基準 6.2 エ）

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。

※「クラウドサービスの特性」についての考え方

クラウドサービスを利用した情報システムは、従来のオンプレミスによる情報システムと比べ、主に以下の特性がある。

- クラウドサービス事業者の用意するコンピューティング資源を多くのクラウド利用者で共有し、その上に各クラウド利用者が利用する情報システムが構築される。そのため、市が情報システムを構築する際のセキュリティ対策のみでなく、クラウドサービス事業者やコンピューティング資源を共有している他のクラウド利用者の情報システムにおいて情報セキュリティインシデントが発生し、その影響を受ける可能性がある。
- クラウド利用者は処理能力やストレージ等のコンピューティング資源を、利用者の操作で追加又は削除することができる。しかし、クラウドサービス事業者の用意する資源の不足等が発生した場合に即座に資源の追加ができず、可用性を損なう可能性がある。
- クラウドサービス事業者はコンピューティング資源を分散して配置することが可能であり、海外に配置されている可能性がある。

（留意事項）

情報管理者は、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。

・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
・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
・**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
・クラウドサービス上の**脆弱性対策**の実施内容の確認
・クラウドサービス上の情報に係る復旧時点目標（BPO）等の指標
・クラウドサービス上で取り扱う情報の暗号化
・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
・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

※「アクセスログ等の証跡の保存」についての考え方

クラウドサービス上におけるアクセスログ等の証跡に係る保存期間については、オンプレミスと同様に情報システム又は当該システムに保存される情報の特性に基づき、設定される。ただし、標的型攻撃に関し、攻撃の初期段階から経緯を確認する観点からは、過去の事例を踏まえ、ログは 1 年間以上保存することが望ましい。

なお、記憶媒体に保存する期間については、過去に遡って調査する期間や頻度、どの程度のコストをログの保存にかけられるかを考慮して決定する。

※「クラウドサービスの委託先による情報の管理・保管」についての考え方

情報管理上の問題として、仮に情報がクラウド上にあったとしても、当該情報の責任は利用者である情報オーナーが負うこととなっているため、利用者はクラウドサービス事業者による情報の管理・保存方法について事前に把握する必要がある。

また、クラウドサービス事業者が外部委託先に情報の管理・保管を委託した場合、当該情報が利用者の意図しない場面で二次利用されることも懸念されるため、外部委託先における情報セキュリティ水準や情報の取扱方法に関してクラウドサービス事業者に確認の上、合意しておく必要がある。

※「脆弱性対策」についての考え方

例えば、仮想化技術を用いたマルチテナントの環境において、OS 等の脆弱性に加えてハイパーバイザーを経由して他の利用者が享受するサービスを阻害する脆弱性はクラウドに対するリスクであり、対策を講ずる必要がある。このような脆弱性を発見する方法として、脆弱性発見ツールを用いた手法やペネトレーションテスト等が挙げられる。

※「情報開示請求に対する開示項目や範囲」についての考え方

クラウドサービスに関し、クラウドサービス事業者が一般に公開している内容以上の情報提供について、情報セキュリティ対策や監査の観点から、事前に市とクラウドサービス事業者が協議の上、クラウドサービス事業者が提供する内容の項目や範囲を契約において明記することが必要である。また対象情報の機密性が高い場合、両者間で秘密保持契約（NDA：Non-Disclosure Agreement）を締結するなど必要な情報を講じた上で取得することが求められる。

(5)（管理基準 6.2 オ）

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。

※「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・認証制度の運用状況等から、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」についての考え方

クラウドサービス事業者及び当該サービスの信頼性が十分であることを総合的に判断するためには、クラウドサービスで取り扱う情報の機密性・完全性・可用性が確保されるように、クラウドサービス事業者のセキュリティ対策を含めた経営が安定していること、クラウドやアプリケーションに係るセキュリティ対策が適切に整備され、運用されていること等を評価する必要がある。

このような評価に当たって、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用することが考えられる。その場合、監査や認証等によって保証される対象範囲がクラウドサービス事業者の全部または一部の場合があるので、市が委託するクラウドサービスが当該対象範囲に含まれていることを確認する必要がある。また、監査の場合には、監査項目の網羅性に留意して、重要な監査項目が除かれていないか、監査意見に除外事項（内部統制の不備）が含まれていないかなどを確認する必要がある、さらに、その監査や認証等によっては、クラウドサービス事業者の経営の安定性やサプライチェーンリスク等は上記の評価に含まれてしまうことが考えられるため、これらのリスクについては市が評価する必要がある。

なお、参考となる認証には、ISO/IEC27017 によるクラウドサービス分野における ISMS 認証の国際規格があり、そこでは「クラウドサービス事業者が選択する監査は、一般的には、十分な透明性をもった当該事業者の運用をレビューしたいとする利用者の関心を満たすに足りる手段とする」ことが要求されており、これらの国際規格をクラウ

ドサービス事業者選定の際の要件として活用することも考えられる。その他、日本セキュリティ監査協会のクラウド情報セキュリティ監査やクラウドサービス事業者等のセキュリティに係る内部統制の保証報告等である SOC 報告書（Service Organization Control Report）を活用することも考えられる。特に、SOC 2 ・SOC3 は、米国公認会計士協会が開発した「Trust サービス原則と基準」で定義された「セキュリティ、可用性、処理のインテグリティ、機密保持、プライバシー」の 5 つの原則を適用したものであるため、クラウドサービス事業者及びサービスに対する評価の際の参考となり得る。また、SOC2・SOC3 については、日本公認会計士協会の IT 委員会の実務指針により国内でも同様の保証報告書が制度化されている。ただし、SOC2・SOC3 及び実務指針第 7 号においては、この 5 つの原則の一部のみを選択して実施することができるため、当該監査で選択した原則に「セキュリティ」が含まれていることを保証報告書により確かめる必要がある。

3　クラウドサービスのリスクに関する考察

(1) Dos 攻撃

クラウドサービスはネットワークで提供されるため、Dos 攻撃を受けた場合、すべてのサービスが停止してしまう可能性がある。Dos 攻撃を防御するための仕組がクラウド事業者に依存するため、クラウド利用者は対策を講じることができない。クラウド利用者は、このようにクラウド事業者にしか対応できない問題については、あらかじめクラウド事業者に管理者を確認し、Dos 攻撃のリスクを受容するか検討を要する。

(2) ID 管理

クラウドサービスによっては、クラウド利用者が既に利用している ID 管理とクラウドサービスにおける ID 管理を一元的に実施するためのインタフェースがない場合がある。その場合は、管理者の ID 管理に関する工数が増大し、一貫したセキュリティ対策及び管理を行うにあたってミスが発生する可能性が高くなる。そのためクラウド利用者は、ID 管理の連携ができるクラウドサービスを選ぶか、ID 管理が困難になるリスクを受容するか検討を要する。

(3) アクセスポイント

公衆無線 LAN や携帯電話網の普及によって、様々な場所からクラウドサービスを利用できるようになり、ネットワークにおけるアクセス制御が困難になっている。そのため、クラウド利用者は、アクセスポイントを制御できるクラウドサービスを選ぶか、あらかじめ、利便性は上がるが管理は困難になる、ということを認識してクラウドサービスを利用するリスクを受容するか検討を要する。

(4) アクセス制御

利用するクラウドサービスによっては、あらかじめ定められたアクセス制御が、組織で想定するアクセス権とは異なり、アクセス制御が困難になる場合がある。そのため、クラウド利用者は、アクセス制御が管理できるクラウドサービスを選ぶか、あらかじめ、クラウドサービスが定めたアクセス制御を受入れることによるリスクを受容するか検討を要する。

(5) アプリケーション

主に SaaS で提供されるアプリケーションはデスクトップ上で提供されるアプリケーションと違い、機能が制限されていることがある。例えば、デスクトップ用のアプリケーションデータをインポートした場合にすべての条件が反映されないような場合である。また、クラウドサービスで提供されるアプリケーション同士もデータの互換性が十部であるとはいえない。そのため、クラウド利用者は、互換性の高いクラウドサービスを選択するか、あらかじめ互換性に制限がある、ということを認識してクラウドサービスを利用するリスクを受容するか検討を要する。

(6) インシデント管理

インシデント管理には様々な情報が必要になるが、クラウドサービス利用において自

らが入手できる情報が制限される場合、クラウド利用者が主体となった対応ができなくなる可能性がある。特に、クラウド事業者が考えるインシデントやイベントのレベルと利用者組織のレベルが合致していないことにより、定められた対応がされなかったり、その発生によるビジネスに対する影響が明確にできなかったりする課題がある。そのため、クラウド利用者は、契約時にインシデントやイベントのレベルを合意するか、あらかじめクラウドサービスが定めたインシデントやイベントのレベルを受入れることによるリスクを受容するか検討を要する。

(7) クラウド事業者の事業継続

クラウド事業者が何らかの理由により事業継続が困難となった場合、若しくは、クラウドサービス自体を戦略的に停止することになった場合、そのクラウド事業者が提供するクラウドサービス利用が制限され、クラウドサービス上の情報が利用できなくなり、クラウドサービス上に保存された情報が消失する可能性がある。そのため、クラウド利用者は通常の取引先としての信頼性の確認だけでなく、クラウドサービスを行う事業部の継続性も確認して、クラウドサービスの利用を決定し、また、クラウドサービスの停止はクラウド事業者が決定するというリスクを受容するか検討を要する。

(8) システム運用・保守

クラウドサービスではシステム自体の保守をしなくても良いというのがメリットの一つではあるが、情報セキュリティの観点では業務の委託はできても責任をすべて委譲することはできない。クラウドを利用していない環境でのセキュリティ規程を満足させるために様々な情報が必要になる。

(9) スケールアウト技術

クラウドコンピューティングにおけるスケールアウトという技術により、ハードウェアを仮想的に連携させ処理能力の高いハードウェアを形成することができる。ハードウェア単体における物理的な能力を超えた環境についての機能が十分できないことから、未知のトラブルが発生する可能性がある。新たな技術の導入に伴う未知のリスクは予知し難く、クラウド利用者は、リスク移転（利用料の減額など）が可能か、それともリスクを受容するか検討する。

(10) データセンターの所在

様々な国や場所にデータセンターが設置される場合の、データセンターに従事する従業者の経験やモラルなどによる情報の取扱いの差が、クラウド利用者の懸念事項として挙げられている。様々な国のネットワークの接続性などに伴って、サービスの質などの差による影響が出る可能性が考えられている。そのため、クラウド利用者は、あらかじめデータセンターの所在地の法規の適用にかかわる問題を認識してリスクを受容するかの検討を要する。

(11) データセンターの物理環境

利用者からみたデータセンターのありようは大きく変化していないと考えらえるが、

クラウドサービスを提供するために新たな技術や運用形態（コンテナ式など）を利用したデータセンターが運営されており、クラウド事業者が経験していない問題が発生する可能性がある。クラウド利用者は、新たな技術や運用形態に起因するリスクの移転（利用料の減額など）が可能か、それともリスクを受容するか検討を要する。

(12) ヘルプデスク

海外のクラウドサービスを利用している場合、ヘルプデスクサービスの対応言語が異なり、時差や営業日の違いによってサービス日・時間帯が国内と異なる場合がある。そのため、クラウド利用者は、あらかじめ対応言語や対応時間などにかかわるリスクを受容するか検討を要する。

(13) マルチテナント

一つのプラットフォーム上に複数の契約者が同居することにより、プラットフォームを狙った攻撃が実施された場合に対象ではないほかの契約者にも影響が及ぼされることになる。特にクラウドサービス環境においては、どの契約者とどの契約者が同じシステム内で同居しているがわからないことが問題となる。そのため、クラウド利用者の管理の不備によって引き起こされるリスクについて検討した後、他の契約者の管理不備によって引き起こされるリスクについても検討を要する。

(14) メモリ管理

クラウド事業者では物理的なメモリ管理などが実行できないために、メモリ保護に関するトラブルが発生した場合の問題について、ハードウェアが原因か、仮想化などによる技術的な問題かを切り分けを行うことが難しい。クラウド利用者は、このような技術的なトラブルに対するリスク移転（利用者の減額など）が可能か、それともリスクを受容するか検討を要する。

(15) メンテナンスユーティリティ

システムの状況を知るためのユーティリティが提供されないことによって、情報を適宜入手することができないという課題がある。情報を入手できないことでトラブルの事前判断ができないだけではなく、経営面からみて IT の活用状況がわからないなどの課題もある。そのため、クラウド利用者は、あらかじめ情報の把握が困難になるリスクを受容するか検討を要する。

(16) ライセンス管理

クラウドサービスを前提に作成されていないソフトウェアのライセンス体系により、クラウドサービス上でソフトウェアがどのように利用されているのかを正確に把握できないことがある。そのため、ソフトウェア監査におけるトラブルへ発展することがある。クラウド環境を見越したライセンス体系をもつソフトウェアも増加しており、クラウド利用者は、利用するソフトウェアのライセンスの再確認や、場合によっては契約の再確認を行う。

(17) リカバリー

クラウドサービスを利用して顧客向けサービスを提供しているような企業や組織においては、復旧計画を正確に顧客に知らせることができないという問題が発生する。SLA による復旧予定を通知できる場合はそれを通知するが、それ以外の場合に通知は困難である。また、クラウドサービスが顧客向けサービスの唯一のインタフェースである場合は、通知自体も不可能になるため、クラウド利用者は代替策を講じるか、リスクを受容するか検討を要する。

(18) ログ監視

サーバへのアクセスなどネットワークに関するログを取得することができないクラウドサービスのスキャニングなどが行われていることなど、自らの資産が危機にさらされているかもしれないという事実を知ることが難しく、事前に対策をすることができないという課題がある。そのため、クラウド利用者は、ログ監視と対応を行っているクラウドサービスを選ぶか、あらかじめスキャニングなどの認知は困難である、ということを認識してクラウドサービスを利用するリスクを受容するか検討を要する。

(19) 暗号化

クラウドサービスの多くは SSL/TLS を利用した暗号化通信を選択することができるが、対応していないサービスを提供している事業者や、クラウド事業者内の経路では暗号化通信を行っていない場合もある。そのような場合には、機密データや重要データのやり取りにおいて暗号化を規定しているにもかかわらず、クラウド事業者のネットワーク上でデータが暗号化されないという課題がある。クラウド利用者は、暗号化されないことのリスクを受容するか検討を要する。

(20) 仮想化技術

仮想化環境においては、CPU やメモリなどの利用が物理的に行われた場合とは異なる管理が行われることがある。また、ネットワークやストレージなども仮想化され単一機器と動作が異なる場合もあり、リスクを生む可能性がある。仮想化環境を前提としたアプリケーションの設計が行われていない場合、処理速度が低下するだけではなく、必要以上のコンピュータリソースを使用することで、クラウド本来のメリットであるコスト削減などに寄与しないという問題も考えられる。このような問題に対して、クラウド利用者は、リスク移転（利用料の減額など）が可能か、それともリスクを受容するか検討を要する。

(21) 携帯電話・スマートフォン

携帯電話やスマートフォンは、PC に比べてセキュリティ対策を行うためのオプションが少なく、本格的な運用実績も少ないため、クラウドサービスが携帯電話やスマートフォンから利用できる場合は、トラブルに関する情報や対策についての十分な情報が得られないという課題がある。そのため、クラウド利用者は、携帯電話やスマートフォンによる利用を制御できるクラウドサービスを選ぶか、あらかじめ利便性は上がるが管理は困難になるということを認識してリスクを受容するか検討を要する。

(22) 最大許容停止時間

システムの最大許容停止時間について明確な指針が必要になる。最大許容停止時間は、クラウド事業者が定めるものであり、クラウド利用者は、クラウド事業者の定めに応じて復旧を待たねばならない。サービスにおける稼働率は SLA などの契約で定められるが、クラウド利用者は、最大許容停止時間の実態を確認するためにも過去のトラブルの状況などを問い合せ、これまでにどの程度サービスが停止したことがあるか、クラウド事業者の改善策によってその問題が解決しているかなどの確認を要する。

(23) 残存データ

メモリ上、ハードディスク上にデータが残ってしまった場合の処理について仮想化された環境で十分にこれらを制御することができるかどうか、可視化できない問題がある。そのため、クラウド利用者としては、クラウドサービスにおけるこれらの残存データの処理方法についてクラウド事業者が講じている技術的な処理方法についての情報を得るか、残存メモリ・残存オブジェクトが発生するリスクを受容するか検討を要する。

(24) 実行環境の制限

クラウドサービスでは提供される実行環境に制限がある場合が多い。アプリケーションによっては必要なライブラリが使えないことによって、動作しないことも考えられる。PaaS ベンダーによっては独自の開発言語やビジュアルエディタのみによる開発環境の提供により、他社のサービスを利用できないという問題が発生する。そのため、クラウド利用者は、汎用性のある実行環境を提供するクラウドサービスを選択するか、あらかじめ実行環境に制限があるリスクを受容するか検討を要する。

(25) 従量課金を利用した攻撃

クラウドサービスの契約形態によっては、利用したリソースに応じた使用料が課金される。この特性を利用して、処理を必要以上に増加させる攻撃が外部から行われることがある。DoS 攻撃のようにサービスの利用を妨げるのではなく、経済的に事業継続を不可能にする攻撃である。このような経済的な攻撃を EDoS（Economic Denial of Sustainability）と呼ぶことがある。クラウド利用者は、EDoS 攻撃により発生した使用料に関してクラウド事業者とあらかじめ取決めを交わすか検討を要する。

(26) 接続性

クラウドサービスは国内だけではなく、海外でも展開され、国内からの利用も増えている。国内外を問わず、事業者は様々な場所にクラウドサービスを提供するためのデータセンターを展開しており、かつそれらが連携して運用されている。そのため、ネットワーク構成が複雑になり、接続の信頼性を把握することができないという課題がある。そのため、クラウド利用者は、接続性にかかわるリスクの移転（利用料の減額など）が可能か、それともリスクを受容するか検討を要する。

(27) 相互運用性

クラウドサービスに関連する様々な標準化（技術、データ形式、サービス形態など）

が行われていない現状では、アプリケーションのデータや作成されたシステムのイメージデータなどが、他のサービスで利用できなかったり、システム同士の連携ができなかったりという問題が発生する可能性がある。そのため、クラウド利用者は、相互連携性の高いクラウドサービスを選択するか、あらかじめ相互運用性にかかわるリスクを受容するか検討を要する。

(28) 中間者攻撃

データセンターが様々な場所で展開され、かつ連携していることを前提とした場合、１対１の接続の場合に比べて中間者攻撃を受けやすくなっている。また、マッシュアップなどによってサービスが構成されている場合などは更に攻撃の機会が増えると考えられる。このような中間者攻撃に起因する被害の発生について、クラウド利用者は、リスク移転（利用料の減額など）が可能か、それともリスクを受容するか検討を要する。

(29) 分散管理

クラウドサービスでは冗長性や拡張性がそのメリットとして挙げられているが、反面これらのメリットを実現するための分散管理などの管理手法が、対象としている情報及びシステムの構造を複雑にし、クラウド利用者からの可視化を妨げており、情報やシステムの一元管理を実施しにくくしている。そのため、クラウド利用者は、クラウド事業者が使用する技術によっては、データの所在を明確に把握できないことによるリスクを受容するか検討を要する。

４　クラウドサービスの導入に関する手続

(1) 準備段階

クラウドサービスの利用検討に先立ち、対象となるサービス・業務及び情報といった以下の事項を可能な限り明確化する。

① 業務の基本属性

- 主なサービス利用者（市民向けのサービスか、職員向けのサービスか）及びその利用者の詳細
- インターネット利用を前提とした業務か否か
- 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
- 他のサービスやシステムとの連携

② 必要なサービスレベル

- サービス提供時間
- 障害発生時の復旧許容時間
- 災害対策の要否等

③ サービス・業務の定常性

- 定常的なサービス・業務か、試行的又は一時的なサービス・業務か

④ 業務量

- 業務処理量の総量、単位時間当たりの処理量の予測
- 業務処理量の変動（増加・減少、ピーク特性等）予測

⑤ 取り扱う情報

- 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）、取扱制限の有無

(2) クラウドサービスの選定基準

- 十分な稼働実績を有し、運用の自動化、サービスの高度化、情報セキュリティの強化、新機能の追加等に積極的かつ継続的な投資が行われ、サービス終了のリスクが低いクラウドサービスを選定するものとする。
- 「２　クラウドサービスの利用に係る遵守事項」を満たすクラウドサービスを選定するものとする。
- クラウドセキュリティ認証等を必須とする。
- クラウドサービスに保存されるデータの可用性の観点から、国内法及び条約が適用される国内データセンター及び日本に裁判管轄権があるクラウドサービスを採用候補とするものとする。

(3) クラウドサービスに係るセキュリティポリシー

- 行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産をパブリッククラウド上で扱わないものとする。
- クラウドセキュリティ認証等の認証基準、監査フレームワークの監査報告書の活

用や個別の調査等により、クラウドサービス提供者から提供されているサービスが本市の情報セキュリティポリシーを満たしていることを確認するものとする。

- クラウドサービス利用時の伝送路は暗号化するものとする。また、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。データの暗号化に使用する鍵については、クラウドサービス提供者側よりも利用者側で管理することが望ましく、選択可能な場合は利用者側で鍵管理が可能な暗号機能を選ぶものとする。
- マイナンバー利用事務系の情報をパブリッククラウド上で扱わないものとする。（対策基準 5.1 ア）
- 機密性 2 以上の情報に係るパブリッククラウドとの通信は、閉域イーサネット、専用線、IP-VPN 等を利用することとする。（対策基準 6.3.4）（管理基準 3.3.2）
  なお、インターネット VPN については、一定の基準を満たしたものについて利用が認められることがある。また、Web 会議・監視カメラ等の映像通信サービスや特定用途機器との通信については公衆回線(SSL/TLS 通信)の利用が可能である。

(4) クラウドサービスの選定方法

- 情報管理者が、クラウドサービスの導入にあたり、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・客観的に判断する際の手続として、当面の間、情報セキュリティ管理者（企画調整局情報化戦略部情報政策担当課長）を通じて CIO 補佐官に企画段階、予算要求段階で協議を行い、CIO 補佐官の関与の下で検討するものとする。

(5) クラウドサービスの利用

- データバックアップは、クラウドサービスの全体的な災害や障害に備え、クラウドサービスの外部でも保管することが望ましい。
- 将来、他のクラウドサービスに移行可能となるように、データ移行の手段を情報システムの要件定義に当初から考慮しておくものとする。
- 情報システムの運用において管理に必要なログの種類とクラウドサービス上取得できるか否か、その際の利用料金等をあらかじめ確認しておくものとする。

(6) 選定方法の例外

- LGWAN-ASP（地方公共団体間の共同利用を目的に行政専用のセキュアなネットワーク（LGWAN）を利用したアプリケーションやコンテンツ、ホスティングサービスで、地方公共団体情報システム機構（Ｊ－Ｌｉｓ）の審査を経て供用しているクラウドサービス）を導入する場合は、本項第 2 号及び第 4 号の選定基準及び選定方法を適用しない。
- 監視カメラ等の映像情報をクラウド上のデータセンターに保存する場合において、「5　クラウドサービス調達仕様書中、データセンターの非機能要件に関する記載例」の各仕様を満たすものは、本項第 4 号の選定方法を適用しない。

(7) セキュリティ評価制度の運用開始後のクラウドサービスの選定方法

- 政府情報システムにおけるクラウドサービスの安全性評価及びクラウドサービスリストへの登録制度（「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組み」でいう安全性評価及び登録制度のことをいう。）を地方公共団体が活用できるスキームが構築された後にクラウドサービスを選定する場合は、原則として公表される登録クラウドサービスリストの中からクラウドサービスを選定することとし、同リストの中から選定が困難なときは本項第 2 号及び第 4 号の選定基準及び選定方法によるものとする。
- 登録リストの中からクラウドサービスを選定する場合は、本項第 2 号及び第 4 号の選定基準及び選定方法を適用しない。

5　クラウドサービス調達仕様書中、データセンターの非機能要件に関する記載例

（監視カメラ等の映像情報をクラウド上のデータセンターに保存する場合の例）

1．利用条件

本業務の実施にあたっては、本調達仕様書の要件並びに以下の利用条件を満たすこと。

1．1　クラウドサービス提供条件

クラウドサービスが具備しているべき条件については「別紙　クラウドサービス要件」のとおりとする。

1．2　サポートに関する条件【推奨事項】

サポートの内容は「クラウドサポートレベル」のとおり。なお、技術サポートへのアクセスはすべてのアカウントにおいて可能であること。

クラウドサポートレベル

要件	内容
サービス受付窓口	日本語対応（日本時間平日 9:00-18:00）
技術サポートへのアクセス	電話、チャット、メール（24 時間年中無休）
緊急度 / 初回応答時間	発生中の障害(影響大)　1 時間以内 発生中の障害　4 時間以内 障害/開発中の急ぎの問い合わせ　12 時間以内 通常の問い合わせ/機能要望　24 時間以内

別紙　クラウドサービス要件

区分	要件
セキュリティ対策・体制	・サービス提供業務の遂行のために提供する情報（契約等の手続に付随してクラウドサービス事業者が知りうる利用者情報等）を、サービス提供業務の遂行目的外で利用しないこと。情報の目的外利用の禁止に対する遵守（義務）の表明をすること。
	・情報セキュリティインシデントが発生した場合に、被害を最小限に食い止めるための対処方法（対処手順、責任分界、対処体制等）について提示すること。 ・障害や情報セキュリティインシデントの発生、監査結果等によって、情報セキュリティ対策の履行が不十分であると認められた場合の対処（改善の実施等）方法について提示すること。

	・以下の情報提供をすること。証明する資料を提出すること。 -サービス提供事業の実施場所（事務所、運用場所）（地域（リージョン）が特定できるようにすること） -メインセンタ、サブセンタについて、物理的に距離が離れた 2 拠点以上で冗長構成されていること【推奨事項】
資格・認証	・サービス提供を行う組織が、ISO/IEC 27001：2013 認証を取得していること。 ・サービス提供を行う組織が、ISO/IEC 27017：2015 認証を取得していること。【推奨事項】
データの所在・適用法と裁判管轄	・サービス上のユーザ所有データ（バックアップデータを含む。）の所在地が日本国内に限定できること。 ・準拠法、裁判管轄を国内に指定できること。
	・データの所有権、管理権は市が保有すること。
サービスレベル	・クラウドサービス事業者との間の管理境界や責任分界を明確にすること。
	・クラウドは正式リリースのサービスを提供すること。
	・可用性について、サービスレベルを提示すること。
	・以下の事前通知の「事前期間」とその「通知方法」について提示すること。事前通知については早期に通知されることが望ましい。また、他にも業務継続性の観点で効果的な通知対象があればそれを提示すること。 -サービスの中断（中止） -クラウドサービス契約の解除
ログ取得	・クラウドサービス上におけるアクセスログ等の証跡に係る保存期間について、1 年間以上の保存が可能であること。その手法について提示すること。
脆弱性対策	・クラウドサービス上の脆弱性を発見する方法があり、実施可能であること。その手法について提示すること。
データ消去	・データを消去する際は、ISO27001 に準拠してデータを復元できないように電子的に完全に消去又は廃棄すること。またデータ消去について第三者の監査機関による監査を受けた内容を提供することが可能であること。

参考 引用文献

- 神戸市情報セキュリティ対策基準
- 物理的・技術的セキュリティ管理基準
- 政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）（平成 30 年 7 月 25 日 内閣官房内閣サイバーセキュリティセンター）
- 政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）（平成 30 年 7 月 25 日 サイバーセキュリティ戦略本部）
- 政府情報システムにおけるクラウドサービスの利用に係る基本方針（2018 年 6 月 7 日 各府省情報化総括責任者（CIO）連絡会議決定）
- クラウドサービス提供における情報セキュリティ対策ガイドライン（第 2 版）（平成 30 年 7 月 総務省）
- クラウドサービス利用のための情報セキュリティマネジメントガイドライン（2013 年度版 経済産業省）
- クラウドサービスの安全性評価に関する検討会とりまとめ（令和 2 年 1 月 クラウドサービスの安全性評価に関する検討会）
- 政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて（令和 2 年 1 月 30 日 サイバーセキュリティ戦略本部決定）