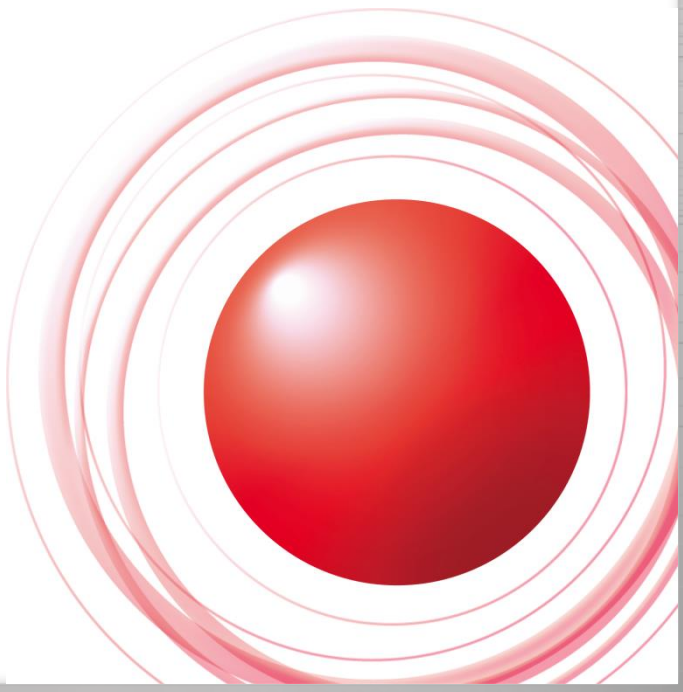
政府機関等の情報セキュリティ対策のための統一基準群に対する情報提供(IIJ GIOインフラストラクチャーP2)

IIJ
Internet Initiative Japan



Ongoing Innovation

本資料について/目次

本資料について

本資料は「政府機関等の情報セキュリティ対策のための統一基準群（平成28年度版）(政府機関の情報セキュリティ対策のための統一基準及び府省庁対策基準策定のためのガイドライン)」のうち、4.1.4 クラウドサービスの利用に対して、IIJ GIOインフラストラクチャーP2について必要な情報を提供する事を目的に作成しています。

目次

- **政府機関等の情報セキュリティ対策のための統一基準群 ～4.1.4 クラウドサービスの利用関連～**
  - 統一基準 遵守事項 4.1.4(1)(a)……p4
  - 統一基準 遵守事項 4.1.4(1)(b)……p5
  - 統一基準 遵守事項 4.1.4(1)(c)……p6
  - 統一基準 遵守事項 4.1.4(1)(c)関連の基本対策事項……p7
  - 統一基準 遵守事項 4.1.4(1)(d)……p8
  - 統一基準 遵守事項 4.1.4(1)(d)関連の基本対策事項……p9,p10
  - 統一基準 遵守事項 4.1.4(1)(e)……p11
- **IIJ GIOインフラストラクチャーP2に関する情報提供**
  - 責任分解点について……p13
  - リソースの分離について……p14
  - 認証取得やSOC報告書の受領について……p15
  - 専属的合意管轄裁判所について……p15
  - サービス設備の設置場所について……p15
  - サプライチェーンについて……p15
  - クラウド上のデータの取り扱いについて……p15
  - サービス廃止ついて……p15
  - サービス設備のキャパシティ管理について……p16
  - 通信の監視について……p16
  - 解約後のデータの取り扱いについて……p16
  - ログの取得について……p16
  - 脆弱性情報への対応について……p16

政府機関等の情報セキュリティ対策のための統一基準群

～4.1.4 クラウドサービスの利用関連～

統一基準 遵守事項 4.1.4(1)(a)

統一基準の遵守事項

(a) 情報システムセキュリティ責任者は、クラウドサービス（民間事業者が提供するものに限らず、政府が自ら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。

府省庁対策基準策定のためのガイドラインの解説(抜粋)

- **遵守事項 4.1.4(1)(a)「情報の取扱いを委ねることの可否」について**

  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半面、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。

    →情報提供「p15,認証取得やSOC報告書の受領について」

  - 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。

    →情報提供「p13,責任分解点について」

  - 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。

    →情報提供「p15,サービス設備の設置場所について」

    →情報提供「p15,専属的合意管轄裁判所について」

  - 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はない。

    →情報提供「p15,サプライチェーンについて」

統一基準 遵守事項 4.1.4(1)(b)

統一基準の遵守事項

(b) 情報システムセキュリティ責任者は、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。

府省庁対策基準策定のためのガイドラインの解説(抜粋)

- **遵守事項 4.1.4(1)(b)「国内法以外の法令が適用されるリスク」について**

  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政府機関のデータを含んだまま没収されるなどが考えられる。

→情報提供「p15,サービス設備の設置場所について」
→情報提供「p15,専属的合意管轄裁判所について」

統一基準 遵守事項 4.1.4(1)(c)

統一基準の遵守事項

(c) 情報システムセキュリティ責任者は、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。

府省庁対策基準策定のためのガイドラインの解説(抜粋)

解説なし

→情報提供「p15,クラウド上のデータの取り扱いについて」

統一基準 遵守事項 4.1.4(1)(c)関連の基本対策事項

基本対策事項
<4.1.4(1)(c)関連> 4.1.4(1)-1 情報システムセキュリティ責任者は、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。 a) 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 b) 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

府省庁対策基準策定のためのガイドラインの解説(抜粋)

- **基本対策事項 4.1.4(1)-1「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**

  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。

→情報提供「p15,クラウド上のデータの取り扱いについて」
→情報提供「p16,サービス廃止について」

統一基準 遵守事項 4.1.4(1)(d)

統一基準の遵守事項

(d) 情報システムセキュリティ責任者は、**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。

府省庁対策基準策定のためのガイドラインの解説(抜粋)

- **遵守事項 4.1.4(1)(d)「クラウドサービスの特性」について**

  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、府省庁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。

    →情報提供「p14,リソースの分離について」

  - 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減することができる。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。

    →情報提供「p16,サービス設備のキャパシティ管理について」

  - 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。

    →情報提供「p15,サービス設備の設置場所について」

統一基準 遵守事項 4.1.4(1)(d)関連の基本対策事項

基本対策事項

<4.1.4(1)(d)関連>
4.1.4(1)-2 情報システムセキュリティ責任者は、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。

a) 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
b) 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
c) **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
d) クラウドサービス上の**脆弱性対策**の実施内容の確認
e) 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
f) クラウドサービス上で取り扱う情報の暗号化
g) 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
h) **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

→情報提供「p16,通信の監視について」
→情報提供「p15,クラウド上のデータの取り扱いについて」
→情報提供「p16,解約後のデータの取り扱いについて」

府省庁対策基準策定のためのガイドラインの解説(抜粋)

- **基本対策事項 4.1.4(1)-2 a)「アクセスログ等の証跡の保存」について**

　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。

→情報提供「p16,ログの取得について」

統一基準 遵守事項 4.1.4(1)(d)関連の基本対策事項

府省庁対策基準策定のためのガイドラインの解説(抜粋)

- **基本対策事項 4.1.4(1)-2 c)「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**

  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になるため、利用者はクラウドサービス事業者による情報の管理・保管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。

  →情報提供「p15,クラウド上のデータの取り扱いについて」

- **基本対策事項 4.1.4(1)-2 d)「脆弱性対策」について**

  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、脆弱性検査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。

  →情報提供「p16,脆弱性情報への対応について」

- **基本対策事項 4.1.4(1)-2 h)「情報開示請求に対する開示項目や範囲」について**

  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、事前に府省庁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措置を講じた上で取得することが求められる。

  →情報提供「p15,認証取得やSOC報告書の受領について」

統一基準 遵守事項 4.1.4(1)(e)

統一基準の遵守事項

(e) 情報システムセキュリティ責任者は、**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。**

府省庁対策基準策定のためのガイドラインの解説(抜粋)

- **遵守事項 4.1.4(1)(e「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」について**

　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又は一部の場合があるので、政府機関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いないことが考えられるため、これらのリスクについては府省庁において評価する必要がある。

　なお、参考となる認証には、ISO/IEC 27017 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書である SOC 報告書（Service OrganizationControl Report）を活用することも考えられる。特に、SOC2・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。

→情報提供「p15,認証取得やSOC報告書の受領について」

IIJ GIOインフラストラクチャーP2に関する情報提供

IIJ GIOインフラストラクチャーP2に関する情報提供

責任分解点について

IIJ GIOインフラストラクチャーP2は、パブリッククラウドとプライベートクラウドを融合させたクラウドサービスです。仮想サーバ、物理サーバ、仮想化プラットフォームの３つの形態の Infrastracture as a Servicre(IaaS)を提供します。

- **責任分解点**

  各提供形態における責任分解点は、下記の通りとなります。

  ・仮想サーバでは、弊社の責任範囲は仮想サーバより下層、お客様責任範囲は OS より上層となります。

  ・物理サーバでは、弊社の責任範囲は物理サーバより下層、お客様責任範囲は OS より上層となります。

  ・VW シリーズでは、弊社の責任範囲は物理サーバより下層、お客様責任範囲はハイパーバイザより上層となります。

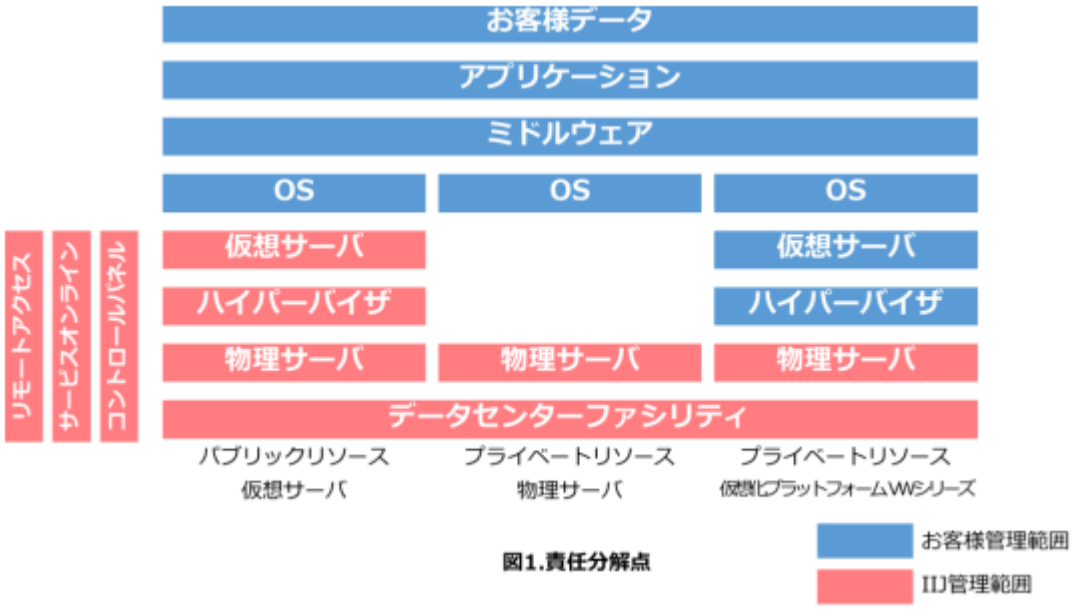


図1.責任分解点

IIJ GIOインフラストラクチャーP2に関する情報提供

リソースの分離について

サーバやストレージ、ネットワークといったリソースを大規模にプールしています。これらに対し、仮想化技術、ネットワークセキュリティ技術を組み合わせることで、サーバやストレージ、ネットワークをお客様ごとに論理的または物理的に分離しています。お客様は、各リソースをお客様専用のリソースのように安全に利用することが可能となっています。

- サーバセキュリティ

  仮想サーバでは、サーバ仮想化技術を用いて、異なる仮想サーバ間に影響を及ぼさないよう、CPUやメモリ、ネットワークのリソースを分離しています。物理サーバおよび仮想化プラットフォームVWシリーズでは、物理サーバ単位での提供によりリソースを分離しています。

- ストレージセキュリティ

  お客様毎にアサインしたストレージボリュームを、お客様毎に分離されたネットワークまたは仮想サーバに1対1で認識されるように制御しています。そのため、他のお客さまから参照されることはありません。

- ネットワークセキュリティ

  ネットワーク仮想化技術を使用し、全て個別のネットワークとしてネットワークセグメントをご提供します。他のお客様のネットワークと分離することにより、高い機密性を確保しています。
  なお、パブリックリソースのグローバルネットワークにおいては、以下の対策を実施することで、お客様同士でのセキュリティインシデントに備えています。

  ・アドレス強制によるセキュリティ対策
  仮想サーバのなりすまし等を防ぐためのセキュリティ対策をしております。契約時に仮想サーバに割り当てられるMACアドレスとIPアドレスが強制されます。割り当てられたアドレス以外を利用しようとするとネットワークの疎通が失われ、通信ができなくなる仕組みになっています。

  ・様々なセキュリティフィルタの適用
  ARP偽造攻撃やブロードキャストを利用した飽和攻撃などを防ぐため、低レイヤーにおける一部プロトコルにフィルターを適用しています。不正利用が疑われるトラフィックにのみ影響を及ぼすもので、通常の利用には問題ありません。

IIJ GIOインフラストラクチャーP2に関する情報提供

認証取得やSOC報告書の受領について

IIJ GIOインフラストラクチャーP2ではSOC1 Type2報告書やSOC2 type2報告書(可用性・セキュリティ)を受領しており、情報を提供する事が可能です。また、クラウドセキュリティの国際標準規格であるISO/IEC 27017:2015の認証取得をしており、要求事項に対する対応としてホワイトペーパーにて情報公開も実施しております。詳細は下記をご参照ください。
<IIJ GIO インフラストラクチャーP2 の ISO/IEC 27017に基づくセキュリティ要求事項への取り組み>
https://www.iij.ad.jp/GIO/security/iso_iec_27017_wp.pdf
なお、IIJ GIOインフラストラクチャーP2のサービス仕様等についてはコーポレートサイトのサービスページやオンラインマニュアルを公開しております。詳細は下記をご参照ください。
<コーポレートサイト サービスページ：IIJ GIOインフラストラクチャーP2>
https://www.iij.ad.jp/biz/p2/

専属的合意管轄裁判所について

IIJ GIOインフラストラクチャーP2はIIJインターネットサービス契約約款に基づき提供いたします。同約款 一般規程 第1章 総則 第7条(専属的合意管轄裁判所)にて当社と契約者の間で訴訟の必要が生じた場合、東京地方裁判所を当社と契約者の第一審の専属的合意管轄裁判所とする旨を定めております。詳細は約款をご参照ください。
<IIJインターネットサービス契約約款>
https://www.iij.ad.jp/svcsol/agreement/

サービス設備の設置場所について

IIJ GIOインフラストラクチャーP2のサービス設備は日本国内のみに設置しております。お客様がクラウド上にデータを保存いただく場合、データの保存先は日本国内となります。

サプライチェーンについて

IIJ GIOインフラストラクチャーP2は他のクラウドサービスの OEM 供給を受けておりません。クラウドサービスの提供の為に必要となる構成要素(データセンターや機器等)の供給については、弊社のセキュリティ方針に沿うようリスク管理しています。

クラウド上のデータの取り扱いについて

IIJ GIOインフラストラクチャーP2ではOSやハイパーバイザーの管理者権限をお渡しする為、クラウド上に保存頂きますデータの取り扱いは、お客様にて実施頂く範囲となります。つきましてはシステム及びデータの移行や暗号化が必要な際はお客様にて実施頂く範囲となります。

IIJ GIOインフラストラクチャーP2に関する情報提供

サービス廃止について

IIJ GIOインフラストラクチャーP2はIIJインターネットサービス契約約款に基づき提供いたします。同約款 一般規程第6章　利用の制限、中止及び停止並びにサービスの廃止第26条　(サービスの廃止)サービスの全部又は一部を廃止するときは、契約者に対し、廃止する日の3ヶ月前までに通知する旨を定めております。詳細は約款をご参照ください。
<IIJインターネットサービス契約約款>
https://www.iij.ad.jp/svcsol/agreement/

サービス設備のキャパシティ管理について

IIJ GIOインフラストラクチャーP2では、サービスの安定稼動を目的にサービス設備のリソース量および稼働状況を管理しており、必要に応じてリソースを追加しております。

通信の監視について

IIJ GIOインフラストラクチャーP2ではクラウド上に構築頂きますシステムに関する通信の監視につきましてはお客様にて実施頂く範囲となります。

解約後のデータの取り扱いについて

IIJ GIOインフラストラクチャーP2の契約解除後、サービスの利用によりお客様がが当社施設設備に存置したデータは弊社にて消去致します。なお、解約前にお客様にてデータの削除を実施頂く事も可能です。

ログの取得について

IIJ GIOインフラストラクチャーP2ではOSやハイパーバイザーの管理者権限をお客様にお渡しする為、クラウド上に構築頂きますシステムの各種ログの取得及び管理についてはお客様にて実施頂く範囲となります。なお、弊社の責任範囲において、サービスの維持管理に必要となるログは適切に取得しております。

脆弱性情報への対応について

弊社では脆弱性情報を常時収集しております。IIJ GIOインフラストラクチャーP2では、収集した情報を元に、サービス設備への影響を評価し、弊社に影響がある場合については、速やかにしております。

IIJ Internet Initiative Japan

Lead Initiative

日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ——IIJはいつもはじまりであり、未来です。

Ongoing Innovation

お問い合わせ先　IIJインフォメーションセンター
TEL：03-5205-4466　（9：30～17：30 土/日/祝日除く）
info@iij.ad.jp

IIJ-GIS034-0001