IIJ Internet Initiative Japan

セキュリティホワイトペーパー

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

改訂履歴

版数	制定/改定日	改定箇所、改定理由	備考
1.0	2016/03/25	新規作成	
1.1	2018/05/09	外部監査の指摘事項に伴う文言修正等	
1.2	2018/06/11	誤字の修正	
1.3	2019/10/01	2019 年監査結果に伴う記載修正	
1.4	2020/11/30	ISMAP への登録に一部文言修正を実施	
1.5	2021/10/13	ISMAP の登録の為の文言修正を実施	
1.6	2022/04/04	内部監査の指摘に伴う、文言の修正	
1.7	2022/08/15	サービス追加に伴う修正等	
1.8	2023/07/27	改訂履歴作成	

目次

はじめに

組織におけるクラウドサービスの利用において、セキュリティへの懸念は必ず取り上げられる問題の一つです。そのような状況の中、2015 年 12 月に、クラウドセキュリティの国際標準規格である ISO/IEC 27017:2015 が発行され、クラウドサービスの利用者と事業者が行うべきセキュリティ管理策が定義されました。

本書では、IIJ GIO インフラストラクチャーP2 および IIJ GIO インフラストラクチャーP2 Gen.2（以下、IIJ GIO P2）における ISO/IEC 27017:2015 への取り組みを解説いたします。IIJ は、ISMS 認証やプライバシーマークなど多くの第三者認証を取得しており、クラウドセキュリティ推進協議会の発足メンバーです。また、セキュリティインシデントに対応する国際組織（FIRST）へ国内企業で初めての加入や、情報セキュリティレベルの向上に寄与する NPO 日本ネットワークセキュリティ協会（JNSA）の役員を務めるなど、安全安心なネットワーク社会の実現に向けて積極的な活動を行ってきました。これらの活動や十数年前からクラウドを運用している豊富な経験、お客様に安心してご利用いただける環境を提供しております。

本書で IIJ GIO P2 におけるクラウドセキュリティの取り組みを知っていただき、IIJ GIO をご活用いただくことで、今後ますますお客様の事業発展のお役に立ちたいと考えております。

なお、本書の内容は作成時点での取組みに基づいて記述しております。内容は変更される場合がございますので、最新の情報は担当営業へご確認くださいますようお願い致します。

IIJ GIO P2 のサービス概要

IIJ GIO 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。

- パブリックリソースおよびフレキシブルサーバリソースでは、弊社の責任範囲は仮想サーバ/マシンより下層、お客様責任範囲は OS より上層となります。
- プライベートリソース 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。
- プライベートリソース 仮想化プラットフォームおよびデディケイテッドサーバリソースでは、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。

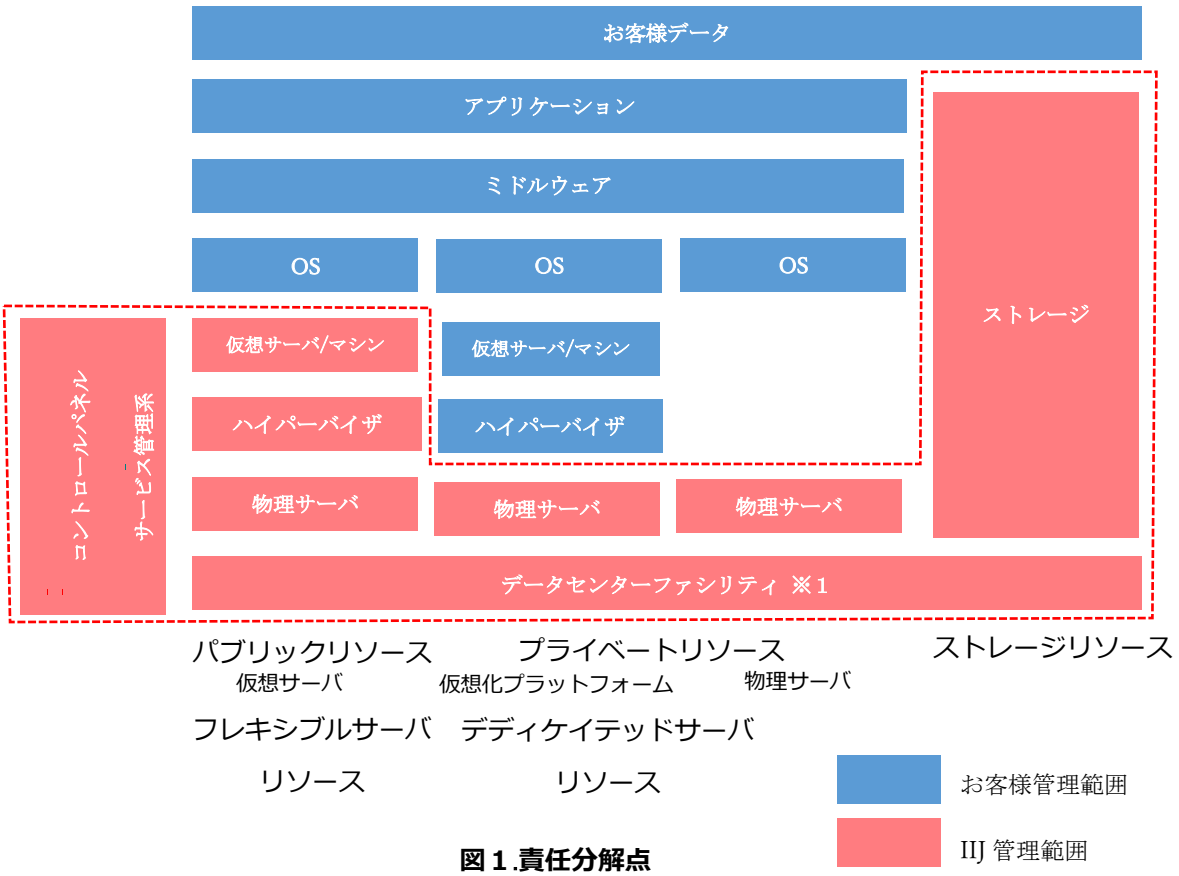


図 1 .責任分解点

■本サービスに関するドキュメント類

IIJ GIO P2 は、IIJ インターネットサービス契約約款に基づき役務提供します。サービス仕様については、サービス詳細資料およびオンラインマニュアルに記載しています(本書では、これらのドキュメントをサービス仕様書と表記しています)。サービスのご利用にあたっての操作方法等については、ご利用の手引きをご用意しています。また、これらのドキュメントの掲載、お客様へのお知らせ、問合せ窓口や運用管理者を管理するために IIJ サービスオンラインおよび P2 ポータルをご用意しております(本書では、これらのサイトをお客様専用のポータルサイトと表記しています)。

IIJ GIO P2 のオンラインマニュアルは以下にて公開しております。

・IIJ 法人向けサービスマニュアル

https://manual.iij.jp/p2/

ISO/IEC27017 の概要

国際標準化機構（ISO）と国際電気標準会議（IEC)が定める情報セキュリティマネジメントの国際規格に ISO/IEC27000 シリーズがあります。ISO/IEC27017 は、このシリーズの 1 つで、2015 年 12 月に発行されたクラウドサービスにおける情報セキュリティマネジメントの指針を記したものになります。

■ISO/IEC27017 の特徴

「ISO/IEC 27002 の管理策に対する追加の実施の手引き」と「クラウドサービスに対する追加の管理策および実施の手引き」ISO/IEC27002 は情報セキュリティマネジメントの汎用的な指針であるのに対し、ISO/IEC27017 はクラウドサービス向けの指針です。ISO/IEC 27002 を前提とした ISO/IEC 27017 には、ISO/IEC 27002 に対して、クラウドサービスに固有の事項を追加されています。具体的に、ISO/IEC27017 には、以下の内容が記載されています。

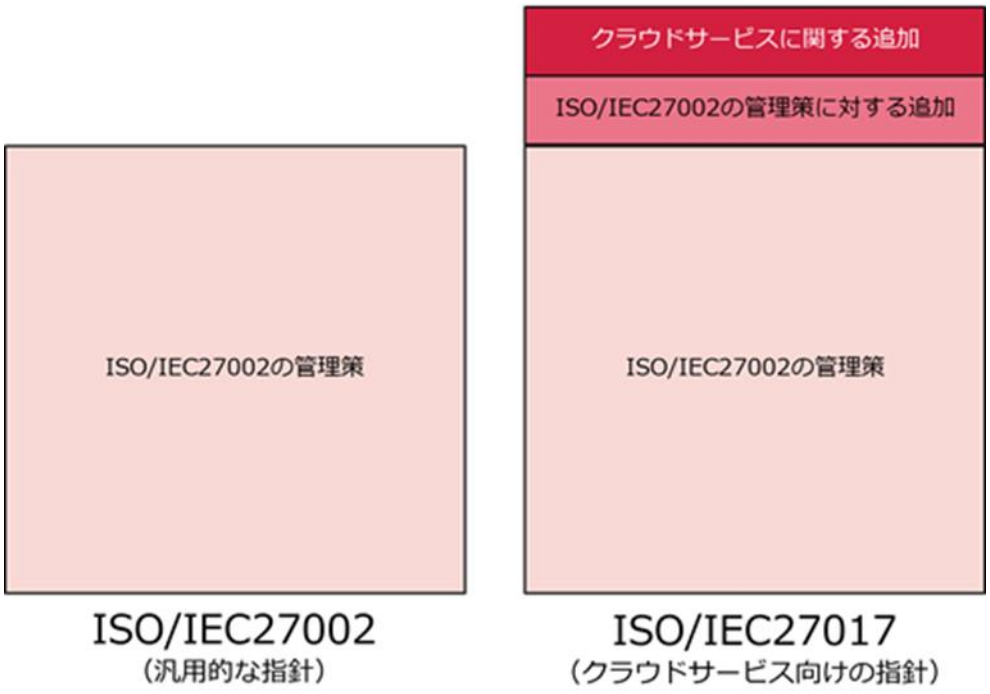


図2. ISO/IEC27002 とISO/IEC27017の体系イメージ

ISO/IEC27017 にて、新たに追加されたクラウドサービス事業者向けの管理策について、IIJ GIO P2 での取り組みを次頁以降に記載しています。

ISO/IEC27017 に対する取り組み

1．情報セキュリティのための方針群

1.1 情報セキュリティのための方針群

ISO/IEC27017 項番：5.1.1

IIJ GIO P2 のサービス運営では以下の方針を定めております。

弊社の情報セキュリティ基本方針(http://www.iij.ad.jp/securitypolicy/index.html)に従い、サービス運営を行います。セキュリティに関して、極めて重要な事項として取り扱います。

また、下記の情報セキュリティ事項を考慮して運営しております。

・クラウドサービス提供業務従事者に関するリスクを特定し対処する。
・仮想化技術などによりマルチテナント及びクラウドサービス利用者を隔離する。
・クラウドサービス提供業務従事者により、クラウドサービスカスタマーデータへのアクセスを制限する。
・クラウドサービスへの管理上のアクセスのための制御手順を定める。
・クラウドサービスの変更はサービス利用者に通知する。
・仮想化技術に固有のリスクを特定し対処する。
・クラウドサービス利用者のデータへのアクセス方法を定め保護する。
・クラウドサービス利用者のアカウントのライフサイクルを管理する。
・クラウドサービスの利用に関る違反が違反した場合の通知、情報共有の方法及び責任範囲を定め、調査及びフォレンジックを支援する。

IIJ GIO P2 では弊社運用担当者がお客様情報資産(お客様にて保存されるデータ)にはアクセスできない仕組みとなっております。なお、マルチテナント形式のサービス品目に関しては仮想化技術やネットワークセキュリティ技術を採用し、お客様システム毎に論理的にセキュアな環境で、リソースを提供しています。また、物理的にセキュアな環境のサービスもご提供し、お客様の要件にあった環境を選択することが可能となっています。

2．情報セキュリティのための組織

2.1 情報セキュリティの役割および責任

ISO/IEC27017 項番：6.1.1

IIJ インターネットサービス契約約款やサービス仕様書にて契約やサービス内容を定義し、サービス提供を実施しております。基本的には OS の管理者権限をお渡しするサービスに関しては OS 以上のレイヤーがお客様責任範囲となり、ハイパーバイザの管理者権限をお渡しするサービスに関してはハイパーバイザ以上のレイヤーがお客様責任範囲となります。

2.2 関係当局との連絡

ISO/IEC27017 項番：6.1.3

弊社の本社所在地は、東京都千代田区富士見 2-10-2 飯田橋グラン・ブルームとなります。なお、IIJ GIO P2 に保存頂くデータの所在は日本国内となります。

2.3 クラウドコンピューティング環境における役割及び責任の共有及び分担

ISO/IEC27017 項番：CLD6.3.1

IIJ インターネットサービス契約約款やサービス仕様書にてサービス内容を定義し、サービス提供を実施しております。また、お問い合わせ窓口はご利用の手引きに記載しております。

3．人的資源のセキュリティ

3.1 情報セキュリティの意識向上、教育及び訓練

ISO/IEC27017 項番：7.2.2

弊社では情報セキュリティ基本方針(http://www.iij.ad.jp/securitypolicy/index.html)を定め、方針に従いサービス運営を行っております。なお、上記規程に、全ての社員に対する教育活動を実施する旨を定めております。

4．資産の管理

4.1 資産目録

ISO/IEC27017 項番：8.1.1

お客様の情報資産(お客様にて保存されるデータ)と弊社がサービスを運営する為の情報は、明確に分離しております。なお、お客様の情報資産(お客様にて保存されるデータ)に関しては、お客様に OS やハイパーバイザの管理者権限をお渡しする為、お客様管理範囲となります。

4.2 情報のラベル付け

ISO/IEC27017 項番：8.2.2

ご契約頂きましたサービス品目の一覧やサービス機能を定めたサービス仕様書をお客様専用のポータルサイトにて閲覧が可能となっています。また、ご契約頂きましたサービス品目毎のサービスコードにて、お客様毎の識別および利用サービスを分類しています。お客様は、ご契約頂きましたサービス品目毎にお客様の資産情報(お客様にて保存されるデータ)を分類することが可能となっています。なお、フレキシブルサーバリソースでは、契約固有のリソースにお客様がラベルを付与する機能をご提供しています。詳細はオンラインマニュアル(IIJ GIO インフラストラクチャーP2 Gen.2 VPC ご利用の手引き/困ったときは/技術情報/セキュリティホワイトペーパー補足資料)をご参照ください。

4.3 クラウドサービスカスタマの資産の除去

ISO/IEC27017 項番：CLD8.1.5

IIJ GIO P2 のサービス解約時に弊社サービス設備に残存したお客様の情報資産は消去いたします。データ消去に関してはサービス Web ページ(https://www.iij.ad.jp/biz/p2/slo/および https://www.iij.ad.jp/biz/p2-gen2/slo.html)に記載をしておりますのでご参照ください。

5．アクセス制御

5.1 ネットワーク及びネットワークサービスへのアクセス

ISO/IEC27017 項番：9.1.2

ネットワークの管理に関しては、社内規定を定め適切に管理しております。

5.2 利用者登録及びネットワークサービスへのアクセス

ISO/IEC27017 項番：9.2.1

お客様専用のポータルサイトにて、ご契約頂きましたサービスに対する運用管理担当者の登録および削除機能を提供しています。

5.3 利用者アクセスの提供

ISO/IEC27017 項番：9.2.2

お客様専用のポータルサイトにて、ご契約頂きましたサービスに対する運用管理担当者の権限管理機能を提供しています。

5.4 特権的アクセス権の管理

ISO/IEC27017 項番：9.2.3

お客様専用のポータルサイトの管理者認証に関しては、ID とパスワードの認証に加え、アクセス元 IP アドレスによる制限を設定する事が可能となっております。

5.5 利用者の秘密認証情報の管理

ISO/IEC27017 項番：9.2.4

お客様専用のポータルサイトをご利用頂く際の運用管理担当者の登録方法についてはメールにてご連絡させて頂いております。

5.6 情報へのアクセス制限

ISO/IEC27017 項番：9.4.1

ご契約頂きましたサービスをご利用頂く際のクラウドサービスへのアクセスの制御に関しては、許可されたお客様のみアクセスできる手段を用いております。

5.7 特権的なユーティリティプログラムの使用

ISO/IEC27017 項番：9.4.4

ご契約頂きましたお客様には、お客様専用のポータルサイトをご提供しています。お客様専用のポータルサイトのご利用においては、ユーザ認証を有し、ご登録されたとアカウントのみご利用いただけます。なお、一部サービスではサービス利用上、お客様責任範囲で一定の権限を付与したユーティリティプログラムを動作させるようお願いする場合があります。詳細はオンラインマニュアル (IIJ GIO インフラストラクチャーP2 Gen.2 VPC ご利用の手引き/困ったときは/技術情報/セキュリティホワイトペーパー補足資料) をご参照ください。

5.8 仮想コンピューティング環境における分離

ISO/IEC27017 項番：CLD9.5.1

仮想化技術やネットワークセキュリティ技術を利用し、サーバやネットワーク、ストレージをお客様ごとに論理的に分離しています。詳細は Appendix をご参照ください。

5.9 仮想マシンの要塞化

ISO/IEC27017 項番：CLD9.5.2

IIJ GIO P2 をご契約頂きました初期状態ではインターネットとの接続性がなく、セキュリティを保った状態でご提供いたします。なお、IIJ GIO P2 では OS やハイパーバイザの管理者権限をお渡しする為、仮想マシンへの適切な技術手段(マルウェア対策やログの取得等)の実施はお客様の管理範囲となります。なお、ご契約頂きましたサービスの初期状態に関しては、サービス仕様書およびご利用の手引きにて開示しております。

6．暗号

6.1 暗号による管理策の利用方針

ISO/IEC27017 項番：10.1.1

基本的にお客様の情報資産(お客様にて保存されるデータ)に関して、弊社にて暗号化を実施することはございません。お客様に OS やハイパーバイザの管理者権限をお渡しするサービスである為、データの暗号化はお客様の実施範囲となりますので、お客様のセキュリティポリシーに合わせたセキュリティ保護を実施して頂く事が可能となっています。

なお、一部のサービス機能および品目では、暗号化機能を提供しています。それらの暗号化機能ついては、サービス仕様書をご参照ください。

6.2 鍵管理

ISO/IEC27017 項番：10.1.2

お客様の情報資産(お客様にて保存されるデータ)に関してはお客様に OS やハイパーバイザの管理者権限をお渡しするサービスである為、データの暗号化はお客様の実施範囲となります。お客様にて暗号化に関するライフサイクルの方針策定が可能となっています。

なお、一部のサービス機能および品目では、暗号化機能を提供しています。それらの暗号化機能ついては、サービス仕様書をご参照ください。

7．物理的及び環境的セキュリティ

7.1 装置のセキュリティを保った処分又は再利用

ISO/IEC27017 項番：11.2.7

設備を再利用、廃棄する際には適切なプロセスで、データの削除や設備の破壊を実施しております。

8．運用のセキュリティ

8.1 変更管理

ISO/IEC27017 項番：12.1.2

サービス内容を変更する場合、影響のあるお客様に対し変更内容をお客様専用のポータルサイトにてご連絡致します。また、メンテナンスを実施する際、お客様に影響のある場合もご連絡しております。

8.2 容量・能力の管理

ISO/IEC27017 項番：12.1.3

安定的にサービスを提供できる仕組みを構築しています。具体的には、リソースの量および稼働状況を管理しています。また、ベストエフォートタイプと専有タイプのようにお客様の要件に合わせ、選択可能なサービスラインアップをご用意しています。

8.3 情報のバックアップ

ISO/IEC27017 項番：12.3.1

お客様システムを直接的にバックアップする機能を付帯していません。バックアップを取得する必要がある場合は、ストレージ機能を提供しておりますのでお客様にて自由にバックアップを構築して頂く事が可能となっています。なお、パブリックストレージ ストレージアーカイブに関してはバックアップ機能を有しております。仕様についてはオンラインマニュアル(IIJ GIO インフラストラクチャーP2 パブリックリソース　サービスマニュアル / B：サービス仕様 / 4.ストレージアーカイブの仕様)、操作についてはオンラインマニュアル(オンラインマニュアル(IIJ GIO インフラストラクチャーP2 パブリックリソース　サービスマニュアル / E：コントロールパネルでの設定方法 / 5.ストレージアーカイブの操作)をご参照ください。また、フレキシブルサーバリソースでは仮想サーバのバックアップを取得するバックアップ機能を提供予定です。

8.4 イベントログの取得

ISO/IEC27017 項番：12.4.1

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適切なログを取得しています。また、お客様責任の範囲においては、OS やハイパーバイザの管理者権限をお渡しするサービスである為、それらの範囲においてお客様自身でログを取得することが可能となっています。

また、IIJ 統合運用管理サービスを利用頂くことにより、きめ細やかなログ監視が可能となっています。

8.5 実務管理者の運用担当者の作業ログ

ISO/IEC27017 項番：12.4.3

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作業ログを取得しております。

8.6 クロックの同期

ISO/IEC27017 項番：12.4.4

弊社では、日本標準時を基にした時刻同期の仕組みを有しています。その弊社の時刻とお客様のシステムの時刻を同期することが可能となっています。

8.7 技術的ぜい弱性の管理

ISO/IEC27017 項番：12.6.1

弊社では脆弱性情報を常時収集しております。収集した情報を元に、サービス設備への影響を評価し、弊社の責任範囲において影響がある場合については、速やかに対応しております。また、お客様に影響しうるインシデントについても、お客様専用のポータルサイトやメールにてお伝えしております。

8.8 実務管理者の運用のセキュリティ

ISO/IEC27017 項番：CLD12.1.5

IIJ GIO P2 をご利用いただくにあたり、必要な操作手順についてはご利用の手引きにて文書化し提供しております。なお、お客様作業による復旧が困難な状況に至った場合に備え、事前に、お客様にてバックアップを取得して頂く必要があります。なお、バックアップの機能については「8.3 情報のバックアップ」に記載の通り、お客様にて適切に構築して頂く必要があります。

8.9 クラウドサービスの監視

ISO/IEC27017 項番：CLD12.4.5

お客様責任範囲の監視につきましては、お客様にて実施頂く必要があります。また、監視機能として IIJ 統合運用管理サービスを組み合わせてご利用頂く事が可能となっています。

9．通信のセキュリティ

9.1 ネットワークの分離

ISO/IEC27017 項番：13.1.3

ネットワークの仮想化技術の使用により、他のお客様と論理的にネットワークを分離し、高い機密性を確保しています。詳細は Appendix をご参照ください。また、サービス運営で必要となる弊社管理ネットワークに関しても、お客様のネットワークと分離しております。

9.2 仮想及び物理ネットワークのセキュリティ管理の整合

ISO/IEC27017 項番：CLD13.1.4

IIJ GIO P2 のサービス提供内容はサービス仕様書に定めています。ネットワークのセキュリティ仕様についてはサービス仕様書をご参照ください。 (パブリックリソースはオンラインマニュアル(IIJ GIO インフラストラクチャーP2 パブリックリソース　サービスマニュアル/ B：サービス仕様 5.ネットワークの仕様 / 5.4 ネットワークの制限事項))を、プライベートリソース、VPC リソース及びフレキシブルサーバリソースはサービス詳細資料をご参照ください。)

１０．システムの取得、開発及び保守

10.1 情報セキュリティ要求事項の分析及び仕様化

ISO/IEC27017 項番：14.1.1

IIJ GIO P2 にてお客様に提供しているセキュリティ機能については、サービス仕様書をご参照ください。

10.2 情報セキュリティに配慮した開発のための方針

ISO/IEC27017 項番：14.2.1

IIJ GIO P2 では、変更管理に関するプロセスを定めてサービス開発・運営を実施しております。変更管理プロセスでは、リスクアセスメントを実施した後、サービスのリリースをしております。

１１．供給者関係

11.1 供給者関係のための情報セキュリティの方針

ISO/IEC27017 項番：15.1.1

OS やハイパーバイザの管理者権限をお客様にお渡しするサービスである為、お客様資産(お客様にて保存されるデータ)へのアクセス権限は、弊社にありません。

11.2 供給者との合意におけるセキュリティの取扱い

ISO/IEC27017 項番：15.1.2

IIJ GIO P2 は IaaS のクラウドサービスとなり、責任分解点は各リソースで異なります。詳細は“IIJ GIO P2 のサービス概要 責任分解点”をご参照下さい。なお、サービス提供内容はサービス仕様書に記載しており、お客様専用のポータルサイトにてダウンロードして頂くことが可能です。

11.3 ICT サプライチェーン

ISO/IEC27017 項番：15.1.3

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。

１２．情報セキュリティインシデント管理

12.1 責任及び手順

ISO/IEC20017 項番：16.1.1

IIJ の責任範囲である、契約者情報やお客様に影響のあるサービス運営上の派生データ等についての機密性・可用性に関する情報セキュリティインシデントが発生した場合には、お客様専用のポータルサイトやメール等にて速やかに報告いたします。なお、責任範囲については“IIJ GIO P2 のサービス概要 責任分界点”をご参照下さい。

12.2 情報セキュリティ事象の報告

ISO/IEC27017 項番：16.1.2

お客様専用のポータルサイトやメールにて、双方向での情報のやり取りを可能とする仕組みを提供しています。

12.3 証拠の収集

ISO/IEC27017 項番：16.1.7

お客様責任範囲における情報セキュリティインシデントに関するログ等の証拠の収集はお客様にて実施頂く範囲となります。弊社責任範囲でのログ等の証拠が必要な場合は、お客様の要望に応じて個別に対応しております。都度、ご相談ください。

１３．順守

13.1 適用法令及び契約上の要求事項の特定

ISO/IEC27017 項番：18.1.1

IIJ GIO P2 のサービス設備は日本国内に設置しております。本サービスをご利用にあたり、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定めております。詳細は IIJ インターネットサービス契約約款 (http://www.iij.ad.jp/svcsol/agreement/)に記載しておりますので、ご確認ください。

13.2 知的財産権

ISO/IEC27017 項番：18.1.2

IIJ GIO P2 上で知的財産権及び権利関係のあるソフトウェアをご利用頂く場合、必要な情報がありましたらお問い合わせください。

13.3 記録の保護

ISO/IEC27017 項番：18.1.3

お客様の契約情報の保護や廃棄については、社内規定に定め、定期的に検査を実施し、適切に管理しております。また、利用については、IIJ インターネットサービス契約約款 第 9 章 契約者情報に定めています。

13.4 暗号化機能に対する規制

ISO/IEC27017 項番：18.1.5

IIJ GIO P2 では、輸出規制の対象となる暗号化の利用はありません。

13.5 情報セキュリティの独立したレビュー

ISO/IEC27017 項番：18.2.1

組織的な取り組みとして弊社では ISMS 認証やプライバシーマークを取得しております。また、IIJ GIO P2 では、ISO/IEC27017 認証に加え、SOC1 報告書や SOC2 報告書(セキュリティ・可用性)を受領しております。

<Appendix>リソースの分離

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

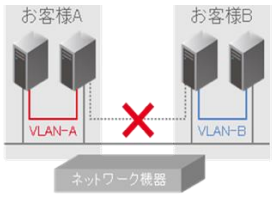
仮想サーバでは、サーバ仮想化技術を用いて、異なる仮想サーバ間に影響を及ぼさないよう、CPU やメモリ、ネットワークのリソースを分離しています。物理サーバおよび仮想化プラットフォーム VW シリーズでは、物理サーバ単位での提供によりリソースを分離しています。

■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。



ネットワーク仮想化の概念図

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 の ISO/IEC 27017 に基づくセキュリティ要求事項への取り組み
株式会社インターネットイニシアティブ
IIJ-GIS014-0009