

セキュリティホワイトペーパー

IIJ プライベートアクセスサービスの 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、改訂理由 | 備考 |
|-------|------------|--|----|
| 1.0 | 2020/10/29 | 制定 | 初版 |
| 1.0.1 | 2020/11/26 | 一部誤記を修正 4.3 資産除去期限の起点を追記 | |
| 1.1 | 2022/07/27 | 情報セキュリティポリシーの更新 コントロールパネルの内容を追記 4.3 資産除去期限の起点を修正 | |
| 1.2 | 2023/10/12 | 提供ドキュメント名変更に伴う更新 責任分界点の文言修正 資産除去期限を明確にする文言修正 | |

目次

| | |
|--------------------------------------|----|
| 目次 | 3 |
| はじめに | 5 |
| IIJ PVA のサービス概要 | 6 |
| ISO/IEC27017 の概要 | 7 |
| ISO/IEC27017 に対する取り組み | 8 |
| 1. 情報セキュリティのための方針群 | 8 |
| 1.1 情報セキュリティのための方針群 | 8 |
| 2. 情報セキュリティのための組織 | 8 |
| 2.1 情報セキュリティの役割および責任 | 8 |
| 2.2 関係当局との連絡 | 9 |
| 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 | 9 |
| 3. 人的資源のセキュリティ | 9 |
| 3.1 情報セキュリティの意識向上、教育及び訓練 | 9 |
| 4. 資産の管理 | 9 |
| 4.1 資産目録 | 9 |
| 4.2 情報のラベル付け | 9 |
| 4.3 クラウドサービスカスタマの資産の除去 | 10 |
| 5. アクセス制御 | 10 |
| 5.1 利用者登録及びネットワークサービスへのアクセス | 10 |
| 5.2 利用者アクセスの提供 | 10 |
| 5.3 特権的アクセス権の管理 | 10 |
| 5.4 利用者の秘密認証情報の管理 | 10 |
| 5.5 情報へのアクセス制限 | 11 |
| 5.6 特権的なユーティリティプログラムの使用 | 11 |
| 5.7 仮想コンピューティング環境における分離 | 11 |
| 5.8 仮想マシンの要塞化 | 11 |
| 6. 暗号 | 11 |
| 6.1 暗号による管理策の利用方針 | 11 |
| 7. 物理的及び環境的セキュリティ | 11 |
| 7.1 装置のセキュリティを保った処分又は再利用 | 11 |
| 8. 運用のセキュリティ | 12 |
| 8.1 変更管理 | 12 |

| | |
|-----------------------------------|----|
| 8.2 容量・能力の管理..... | 12 |
| 8.3 情報のバックアップ..... | 12 |
| 8.4 イベントログの取得..... | 12 |
| 8.5 クロックの同期..... | 12 |
| 8.6 技術的ぜい弱性の管理..... | 12 |
| 8.7 実務管理者の運用のセキュリティ..... | 13 |
| 8.8 クラウドサービスの監視..... | 13 |
| 9. 通信のセキュリティ..... | 13 |
| 9.1 ネットワークの分離..... | 13 |
| 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..... | 13 |
| 10. システムの取得、開発及び保守..... | 14 |
| 10.1 情報セキュリティ要求事項の分析及び仕様化..... | 14 |
| 10.2 情報セキュリティに配慮した開発のための方針..... | 14 |
| 11. 供給者関係..... | 14 |
| 11.1 供給者との合意におけるセキュリティの取扱い..... | 14 |
| 11.2 ICT サプライチェーン..... | 14 |
| 12. 情報セキュリティインシデント管理..... | 14 |
| 12.1 責任及び手順..... | 14 |
| 12.2 情報セキュリティ事象の報告..... | 15 |
| 12.3 証拠の収集..... | 15 |
| 13. 順守..... | 15 |
| 13.1 適用法令及び契約上の要求事項の特定..... | 15 |
| 13.2 知的財産権..... | 15 |
| 13.3 記録の保護..... | 16 |
| 13.4 暗号化機能に対する規制..... | 16 |
| 13.5 情報セキュリティの独立したレビュー..... | 16 |

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プライベートアクセスサービス（以下、IIJ PVA）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 PVA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 PVA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り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せようお願い致します。

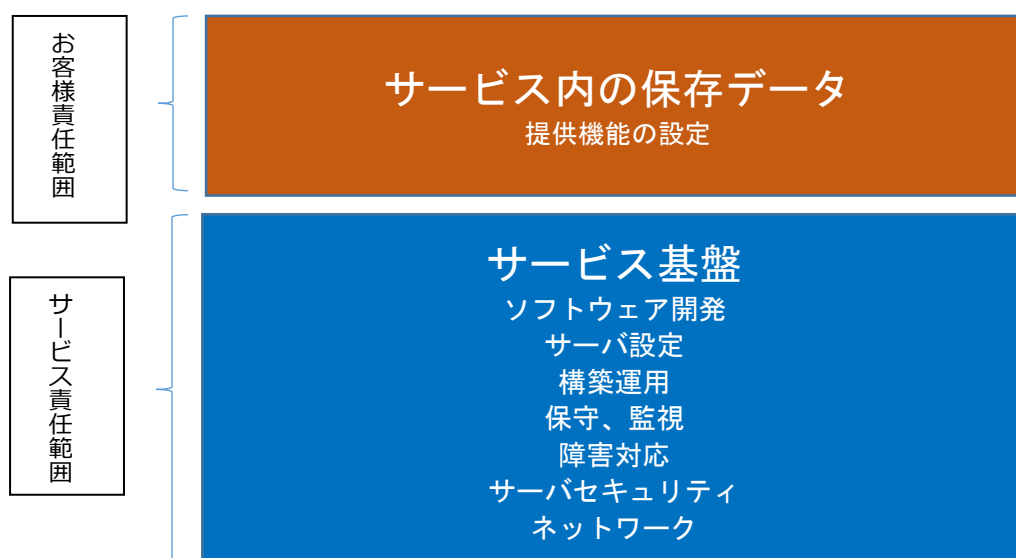
IIJ PVA のサービス概要

IIJ PVA は、顧客拠点やデータセンター内ラックから IIJ プライベートバックボーンサービスへの接続を提供するサービスです。

■責任分界点

IIJ PVA における責任分界点は、下記の通りとなります。

弊社の責任範囲はサービス基盤部分となり、お客様責任範囲は、より上層のサービス内の保存データ（以下、保存データ）となります。



保存データとは、IIJ PVA で提供する機能の設定を指します。

■本サービスに関するドキュメント類

IIJ PVA 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ております。サービス仕様、サービスのご利用にあたっての操作方法等につきましては、仕様書および、マニュアルをご用意しております(本書ではこれらの文書をサービスドキュメントと表記しています)。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担当者を管理するために IIJ サービスオンラインや上記保存データ参照のためのお客様専用のコントロールパネ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)。

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。

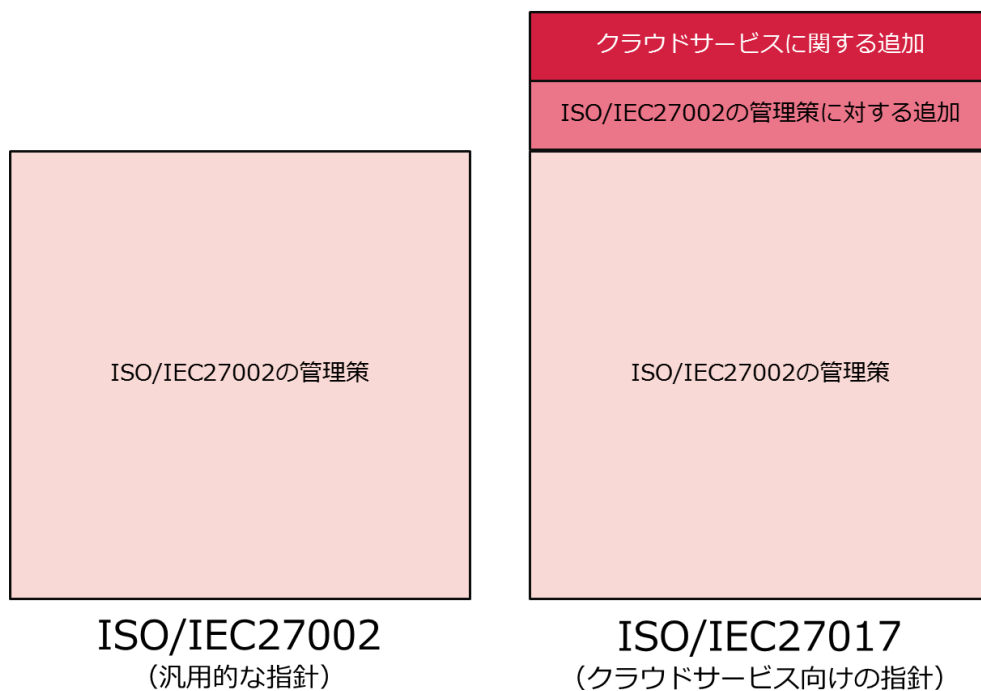


図2. ISO/IEC27002 とISO/IEC27017の体系イメージ

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 PVA 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 PVA では、弊社の情報セキュリティ基本方針に従い、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、サービス運営を行います。

詳細は、IIJ 情報セキュリティ方針(<https://www.ij.ad.jp/securitypolicy/>)をご覧ください。

また、クラウドサービスの提供にあたり、お客様の情報セキュリティ要求を満たすため、次の事項を考慮します。

- 1.クラウドサービスの設計及び実装に適用可能な基本的な情報セキュリティの要求事項を考慮する
- 2.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
- 3.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
- 4.クラウドサービス提供業務従事者による、クラウドサービスカスタマーデータへのアクセスの制限する
- 5.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
- 6.クラウドサービスの変更はサービス利用者に通知する
- 7.仮想化技術に固有のリスクを特定し対処する
- 8.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
- 9.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
- 10.クラウドサービスの利用に関する違反が発生した場合の通知、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

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ドキュメント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。ネットワーク設備などサービス基盤の運用は弊社の責任範囲としてサービスの提供範囲に含まれております。保存データは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。お問い合わせ窓口はサービスドキュメントに記載しております。なお、IIJ PVA に保存された情報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：CLD.6.3.1

IIJ インターネットサービス契約約款やサービスドキュメント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、責任分界点の詳細は、“2.1 情報セキュリティの役割および責任”を参照ください。

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(<https://www.ij.ad.jp/securitypolicy/index.html>)を定め、方針に従いサービスを運営しております。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。

4.2 情報のラベル付け

ISO/IEC27017 項番：8.2.2

契約頂きましたサービスやオプションの一覧やサービス機能を定めたサービスドキュメントが、お客様専用のポータルサイトにて閲覧可能です。また、ご契約頂きましたサービスは、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おります。

また、お客様専用ポータルサイトにおいて、サービスコードに対して自由記入の可能なラベル

欄を用意しております。

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 PVA のサービス解約の際、弊社サービス設備に残存したお客様の情報資産は解約申込の際にお客様が指定する解約日の翌日を起算日（1 日目）として、起算日から 90 日以内に消去しております。

5. アクセス制御

5.1 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、利用者 ID の登録および削除機能を提供しております。

登録、削除に必要な手順、情報はサービスドキュメントに記載しております。

5.2 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、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おります。

権限ごとのアクセス可能な範囲、および権限の変更手順はサービスドキュメントに記載しております。

5.3 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ましては、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や多要素認証を設定する機能を提供しております。

5.4 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利用される際の運用管理担当者および利用者 ID の登録やパスワード変更、再発行方法につきましては、サービスドキュメントに記載しております。

5.5 情報へのアクセス制限

ISO/IEC27017 項番 : 9.4.1

お客様専用のポータルサイトの管理者権限、ユーザ権限等、権限ごとのアクセス可能な範囲につきましては、サービスドキュメントに記載しております。

5.6 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

セキュリティ手順を回避し各種サービス機能の利用を可能とするユーティリティプログラムの提供は行っておりません。

5.7 仮想コンピューティング環境における分離

ISO/IEC27017 項番 : CLD.9.5.1

お客様がアクセスするネットワークと弊社運用担当者が利用する管理ネットワークは分離しています。また、お客様間のデータ分離は、ソフトウェアにて適切に制御しております。

5.8 仮想マシンの要塞化

ISO/IEC27017 項番 : CLD 9.5.2

設備に対する IP アドレスによるアクセス制限の実施、および不要なポート、常駐プログラムは停止しております。

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

お客様専用のポータルサイトの利用にあたっては TLS による暗号化通信が利用できます。また、本サービス設備と送受信するデータを IPsec により暗号化することができます。

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、保存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へのアナウンス掲載、および運用管理担当者宛にメールにて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、ネットワーク設備のリソースの利用状況を管理しております。

8.3 情報のバックアップ

ISO/IEC27017 項番 : 12.3.1

サービスの復旧を目的とした設備情報のバックアップを実施しておりますが、保存データを直接的にバックアップする機能は付帯していません。バックアップを管理する必要がある場合は、お客様にてご取得ください。

8.4 イベントログの取得

ISO/IEC27017 項番 : 12.4.1

サービス設備を経由するお客様データ通信の利用状況を取得し、弊社サービス設備で保管しています。お客様専用のポータルサイトにて公開をしています。

8.5 クロックの同期

ISO/IEC27017 項番 : 12.4.4

弊社では、NTP による時刻同期の仕組みを有しており、日本時間(JST)で管理しています。III PVA で記録される時刻は、すべて時刻同期に基づいて記録されています。

8.6 技術的ぜい弱性の管理

ISO/IEC27017 項番 : 12.6.1

弊社では非公開情報を含め、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は、速やかに対応しております。

8.7 実務管理者の運用のセキュリティ

ISO/IEC27017 項番 : CLD 12.1.5

IIJ PVA を利用頂くにあたり、サービスとして提供している環境をお客様自身で管理操作いただくことはありません。環境の変更等が必要な場合、お客様の依頼に応じて弊社にて変更いたします。

8.8 クラウドサービスの監視

ISO/IEC27017 項番 : CLD 12.4.5

お客様環境からサービス設備との接続点までの到達性監視を提供しており、お客様専用のポータルサイトにおきまして、監視の停止や再開を操作する機能を提供しています。

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

お客様がアクセスするネットワークと弊社運用担当者が利用する管理ネットワークは分離しています。また、ネットワークの仮想化技術を利用し、他のお客様と論理的にネットワークを分離しています。

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 : CLD 13.1.4

本サービスにおいて物理ネットワーク、仮想ネットワークの整合性が取れるよう設計、構築、管理を徹底しています。

お客様毎の仮想ネットワークの契約帯域や実効帯域を踏まえて物理ネットワーク上の帯域リソースを管理しています。

物理ネットワークのポート数、帯域リソースやその他性能等を踏まえて物理ネットワークごとに収容する仮想ネットワークを管理し、増強・増設の計画をしています。

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

情報セキュリティ基本方針、ホワイトペーパーおよびサービスドキュメントに定めております。

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 PVA 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 PVA はクラウドサービスとなり、責任分界点の詳細は、“2.1 情報セキュリティの役割および責任”を参照ください。また情報セキュリティ対策も“2.1 情報セキュリティの役割および責任”の範囲において必要なセキュリティ対策を実施しております。

11.2 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供給は受けておりません。IIJ PVA の提供のため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おります。

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/IEC27017 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にて速やかに報告いたします。

12.2 情報セキュリティ事象の報告

ISO/IEC27017 項番 : 16.1.2

情報セキュリティ事故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。また、お客様からの事象報告はお問い合わせ窓口にて受け付けております。

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 PVA 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社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 (<https://www.ij.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

サービス提供機能で設定された内容や、お客様の送信されたメール、お客様宛のメールはお客様管理下にあります。IIJ PVA お問い合わせ窓口はサービスドキュメントに記載しております。

13.3 記録の保護

ISO/IEC27017 項番 : 18.1.3

8.4 で定めたログを記録し、保管しています。データはお客様ネットワークとは分離された環境で保管され、障害対応で必要になる場合などサービス運用上の用途でのみ利用します。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

お客様専用のポータルサイトでは SSL/TLS の暗号化を使用しております。なお、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。

本書は著作権法上の保護を受けています。

本書の一部あるいは全部について、著作権者からの許諾を得ずに、いかなる方法においても無断で複製、翻案、公衆送信等することは禁じられています。

本内容は予告なく変更されることがあります。

IIJプライベートアクセスサービスの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-PVA004-0004