IIJ Internet Initiative Japan

セキュリティホワイトペーパー

IIJ シンプルバックアップサービスの ISO/IEC 27017 に基づくセキュリティ要求事項への取り組み

第 1.2 版

改訂履歴

版数	制定/改定日	改定箇所、改定理由	備考
1.0	2023/10/17	初版	
1.1	2023/11/17	内部監査指摘事項対応	
1.2	2024/08/26	提供範囲見直しによる対応	

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 シンプルバックアップサービスにおける 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 シンプルバックアップサービス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 シンプルバックアップサービスをご活用いただくことで、今後ますますお客様のセキュリティ強化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 シンプルバックアップサービスの概要

IIJ シンプルバックアップサービスはお客様のサーバイメージやディスク上のデータをバックアップやリストアを行うことができる SaaS 型のバックアップサービスです。

■責任分界点

本サービス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。

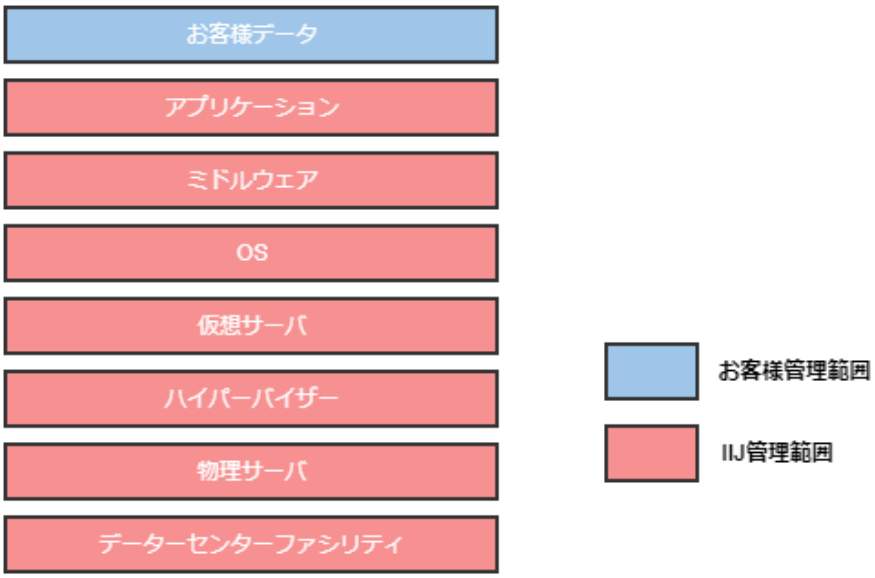

図1. 責任分解点

■本サービスに関するドキュメント類

IIJ シンプルバックアップサービスは、「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」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ドキュメントと表記しています)

サービスのご利用にあたっての操作方法等については、「オンラインマニュアル」をご用意しています(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)。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、及び Acronis コンソー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。

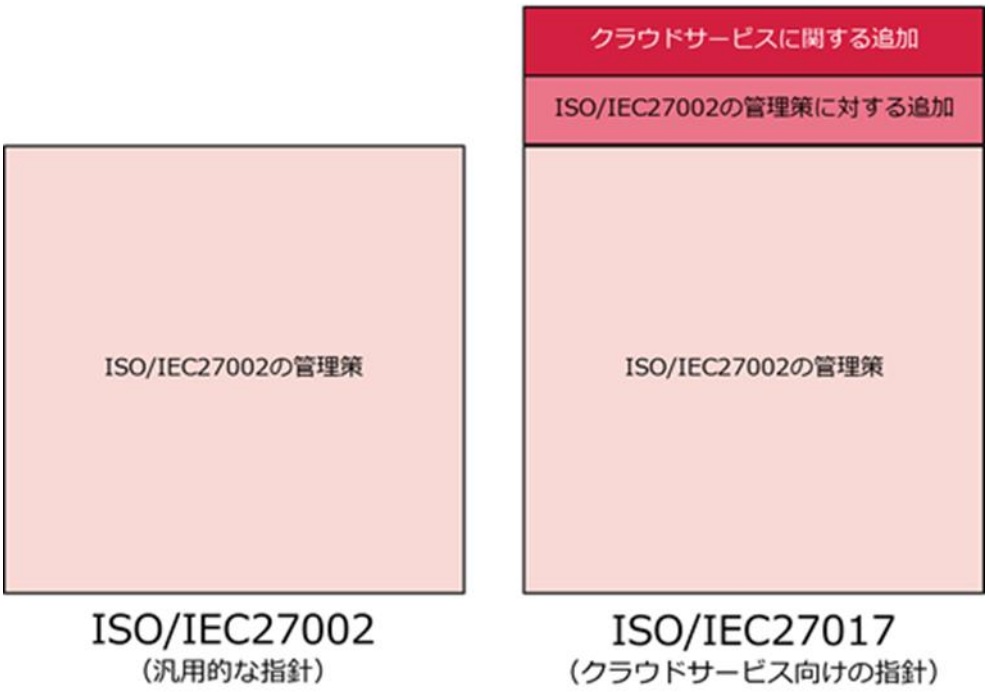

図2. ISO/IEC27002 とISO/IEC27017の体系イメージ

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 シンプルバックアップサービス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 シンプルバックアップサービス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。

・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。

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。アプリケーション、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（お客様データ）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 シンプルバックアップサービスに保存された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、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。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(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。

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、オプション機能を分類しております。

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 シンプルバックアップサービス解約時には、弊社サービス設備に残存したお客様の情報資産は最長 30 日以内に消去いたします。データ消去、並びにサービス運用上に必要な記録（システム出力のログなど）は IIJ シンプルバックアップサービス運用ルールに基づき資産を除去しております。

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の登録および削除機能を提供しています。

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、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。

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お客様運用管理者および利用者 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。

また、IIJ シンプルバックアップサービスは、SaaS（Software as a Service）型のクラウドサービスであることから、提供サービスを利用するための権限のみを付与します。

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おこなっておりません。

5.7 仮想マシンの要塞化

ISO/IEC27017 項番：CLD9.5.2

IIJ シンプルバックアップサービス運用ルールに基づき要塞化をおこなっています。

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(お客様データ)に関しまして、弊社にて暗号化は実施しておりません。

本サービスが提供するコントロールパネル等の通信につきましては、SSL による暗号化通信が利用できます。

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

IIJ シンプルバックアップサービスはクラウドサービスカスタマとしてサービスを構成しクラウドサービスプロバイダーに依存しているため物理装置の資産はありません。

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いたします。

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おります。

また、お客様ご利用設備は、サービス全体で適切なリソース量で提供できるようサイジングを行っています。

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提供しておりません。お客様が設定されたデータに関して、バックアップを行う必要がある場合は、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

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。

お客様専用のポータルサイト等からログをダウンロードすることが可能です。

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

弊社設備（物理・仮想サーバ）は弊社設備の NTP サーバを参照し時刻を同期（日本標準時）しています。

サービス提供している、各種ログについては、時刻同期に基づき記録されています。

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、速やかに対応しております。

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 シンプルバックアップサービスをご利用いただくにあたり、必要な操作手順についてはサービスドキュメントにて文書化し提供しております。

8.9 クラウドサービスの監視

ISO/IEC27017 項番：CLD12.4.5

IIJ シンプルバックアップサービスにおいて弊社管理範囲のネットワークのトラフィック、CPU、メモリ、ディスク使用率、及びシステムログに関する監視は弊社が行っております。これらの情報はお客様には提供しておりません。

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 シンプルバックアップサービスのプライベートゲートウェイオプション機能についてはサービス仕様書をご参照ください。

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

セキュリティホワイトペーパーおよびサービスドキュメントに記載しております。

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

変更管理に関するプロセスを定めてサービス開発・運営を実施し情報セキュリティに配慮しております。

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

お客様から事前に了承をいただいている場合を除き、弊社運用担当者がお客様の情報にアクセスすることはありません。（障害対応やメンテナンス作業で必要となる場合は、稼働確認を行う必要があるためこの限りではありませんが、その場合でも情報へのアクセスは最低限とするように努めます）

また、サービス維持・運用に必要なアクセス権限を厳密に管理します。

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 シンプルバックアップサービスは SaaS のクラウドサービスとなります。詳細は“IIJ シンプルバックアップサービスのサービス概要 責任分界点”をご参照下さい。

11.3 ICT サプライチェーン

ISO/IEC27017 項番：15.1.3

IIJ シンプルバックアップサービスの提供の為に必要となる弊社管理する構成要素(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。また、ピアクラウドサービスプロバイダのクラウドサービスについては情報セキュリティ水準を維持できるように管理します。

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 の責任範囲において確認できたセキュリティインシデントは、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 シンプルバックアップサービスのサービス概要 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

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/ICE27017 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/ICE27017 項番：18.1.1

IIJ シンプルバックアップサービス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(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/ICE27017 項番：18.1.2

IIJ シンプルバックアップサービスをご利用いただく上で知的財産権に関わる問い合わせは、お客様専用のポータルサイトやメールにて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 契約者情報に準じます。

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います。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。

IIJ シンプルバックアップサービスの 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-SBU005-0003