IIJ Internet Initiative Japan

セキュリティホワイトペーパー

IIJ 統合運用管理サービスの ISO/IEC 27017 に基づくセキュリティ要求事項への取り組み

第 1.3 版

改訂履歴

版数	制定/改定日	改定箇所、改定理由	備考
1.0	2021/11/05	初版	
1.1	2022/08/15	・ISMAP 登録に伴う修正/追記	
1.2	2022/08/29	・IIJ 統合運用管理サービスのサービス概要>本サービスに関するドキュメント類にオンラインマニュアルの URL 追加 ・4.2 情報のラベル付け にオンラインマニュアルの詳細追加 ・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 にオンラインマニュアルの詳細追加	
1.3	2023/07/27	・版数、改訂履歴の追加 ・誤字訂正	

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 統合運用管理サービス（以下、本サービス）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頂ける環境を提供しております。

本書で本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頂き、本サービスをご活用頂くことで、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 統合運用管理サービスのサービス概要

本サービスは、システム運用を効率化する SaaS 型サービスです。クラウドからオンプレミスまで、システムから発生する膨大なアラートを自動フィルタリングし、チケットに登録。事前に定めたルールに基づいて必要なアラートだけをシステム運用担当者へお届けします。オペレーションの自動実行、システム監視、ジョブ管理にも対応し、システム運用の効率化をサポートします。

■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。

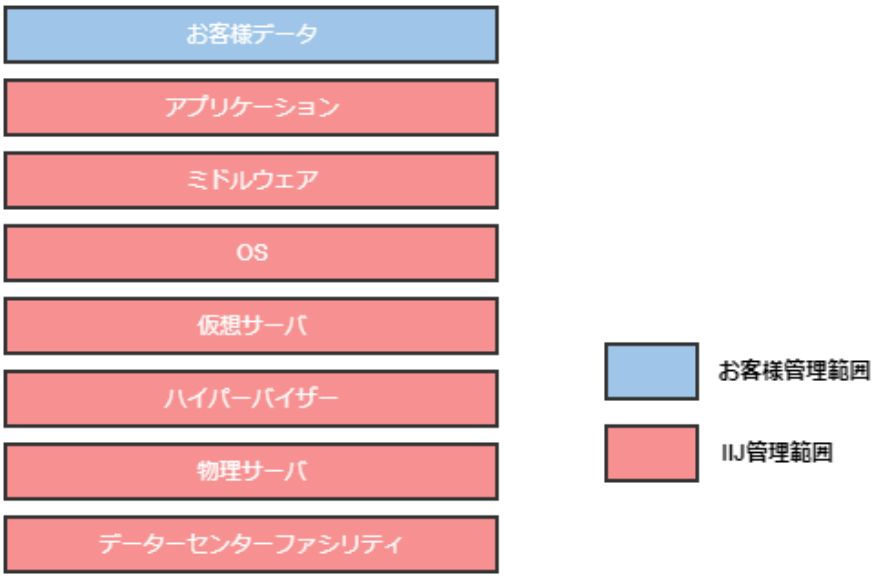

図1. 責任分解点

■本サービスに関するドキュメント類

本サービスは、IIJ ソリューション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、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、及び UOM 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)。

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。

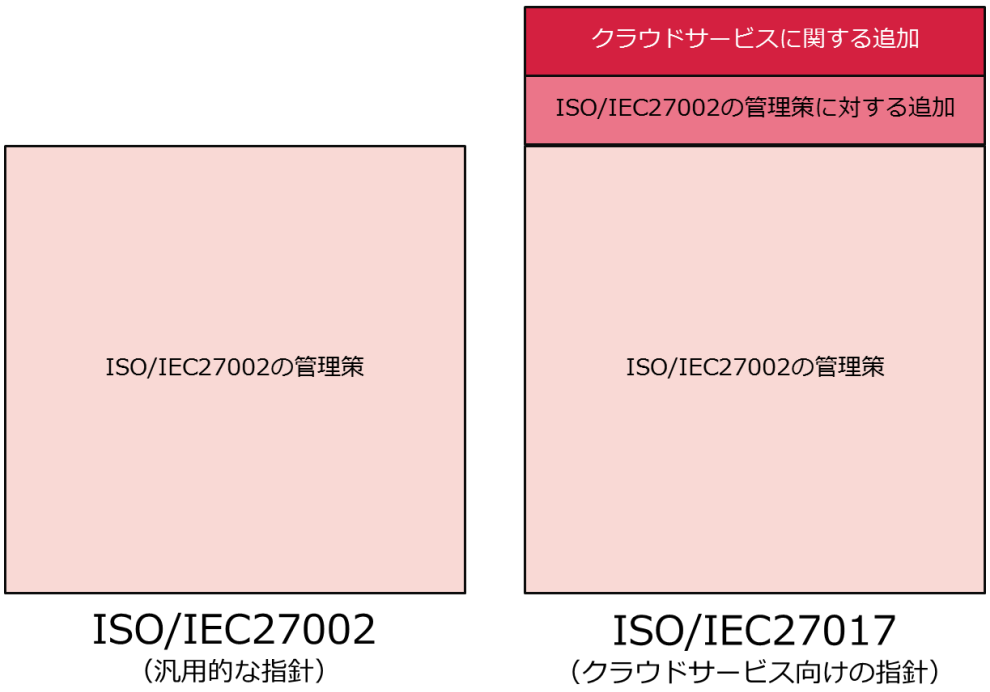

図2. ISO/IEC27002 とISO/IEC27017の体系イメージ

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、本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

本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 ソリューション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。なお、本サービス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 ソリューション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サービス仕様書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。

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を用いてお客様毎の識別、及び利用サービスを分類しています。

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

本サービス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仕様書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、及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

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。

5.8 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

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。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。

5.9 仮想マシンの要塞化

ISO/IEC27017 項番：CLD9.5.2

本サービスの提供に不要なポート、及び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

本サービスとの通信につきましては TLS による暗号化通信が利用できます。お客様の情報資産(お客様にて保存されるデータ)の内、サーバ・ネットワーク機器へのログイン、及びパブリッククラウドと連携するためのアカウント情報を暗号化しております。

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)の内、サーバ・ネットワーク機器へのログインするための鍵情報を暗号化しております。

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、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、及び稼働状況を管理しています。

8.3 情報のバックアップ

ISO/IEC27017 項番：12.3.1

本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

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においてアクセスログを提供しております。

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おります。本サービスでは時刻同期に基づいてログを記録しております。

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

本サービスをご利用頂くにあたり、必要な操作手順はご利用の手引きとし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

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。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。

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

本サービスのプライベート接続サービス提供機能、及びネットワークの通信制御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

本サービス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

本サービスでは、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

サービス仕様書に定める“お客様から提供して頂く情報”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において、稼働確認を行う必要がある場合はこの限りではありませんが、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

本サービスの責任分界点の詳細は、“IIJ 統合運用管理サービスのサービス概要 責任分界点”をご参照ください。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参照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

本サービス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 統合運用管理サービスのサービス概要 責任分界点”をご参照ください。

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

本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。本サービスのご利用にあたり、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 ソリューションサービス契約約款 (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

サービス提供機能で設定された内容はお客様管理下にあります。本サービスのお問い合わせ窓口はサービス仕様書に記載しております。

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。また、本サービスでは、SOC1 報告書を受領しております。

IIJ 統合運用管理サービスの 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-UOM037-0004