IIJ Internet Initiative Japan

セキュリティホワイトペーパー

IIJ DDoSプロテクションサービスのISO/IEC 27017に基づくセキュリティ要求事項への取り組み

第1.7版

改訂履歴

版数	制定/改定日	改訂箇所、改定理由	備考
1.1	2020/12/01	初版	
1.2	2021/05/11	・認証制度名称の誤記訂正	
1.3	2021/11/25	・「仮想マシンの要塞化」にて要塞化の内容を明記 ・「記録の保護」にて月次報告書の掲載期間、解約後のデータ削除について明記 ・「イベントログの取得」にて月次報告書の掲載期間を追記	
1.4	2022/09/22	・「改訂履歴」を追記 ・「5.アクセス制御」「5.1 利用者登録及び登録削除」の文言の訂正 ・「8.運用のセキュリティ」「8.9 クラウドサービスの監視」に情報提供について追記	
1.5	2023/08/30	・「ご利用の手引き」が「マニュアル」に名称変更したことに対応 ・「詳細資料」が「仕様書」に名称変更したことに対応 ・「8.運用のセキュリティ」「8.4 イベントログの取得」の文章を訂正	
1.6	2024/11/14	・1.1 情報セキュリティのための方針群 変更	
1.7	2025/6/26	・11.3 ICT サプライチェーンの内容を変更	

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 DDoS プロテクションサービスにおける 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（JASA）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 CSIRT の国際組織である FIRST（Forum of Incident Response and Security Teams）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 DDoS プロテクション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、サービスの利用を通して、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。

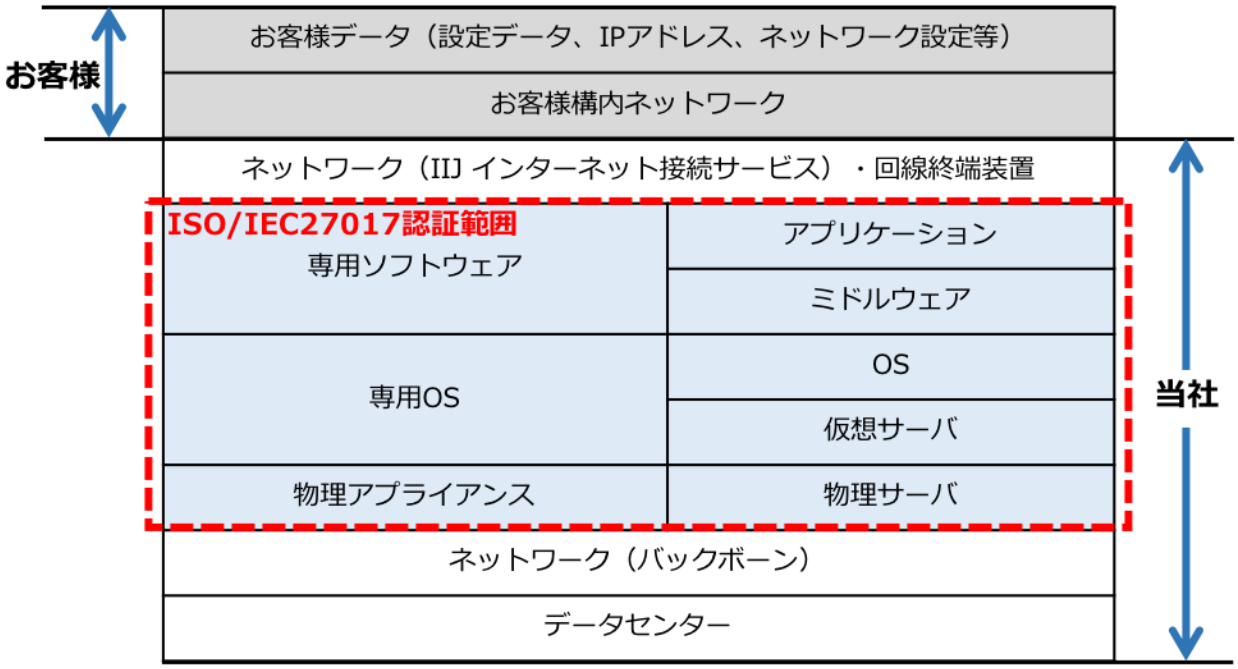
なお、本書の内容は作成時点での取り組みに基づいて記述しております。内容は変更される場合がございますので、最新の情報は担当営業へご確認くださいますようお願い致します。

IIJ DDoS プロテクションサービスの概要

IIJ DDoS プロテクションサービスは、サービス不能を狙った大規模な DDoS 攻撃からネットワークシステムを守るサービスです。基本機能として、トラフィックアノマリ検知、自動防御およびそのレポート、セキュリティイベント監視、通信傾向自動学習を提供し、オプション機能として、常時防御、設定値見直しのための通信傾向再学習によるレポート等を提供しています。

■責任分界点

管理責任範囲は、下記の通りとなります。



■本サービスに関するドキュメント類

IIJ DDoS プロテクションサービスは、「IIJ インターネットサービス契約約款」と「個別規程 IIJ DDoS プロテクションサービス」に基づき役務提供します。サービス仕様については、「サービス仕様書」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、「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、お問い合わ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及び実施の手引き」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。

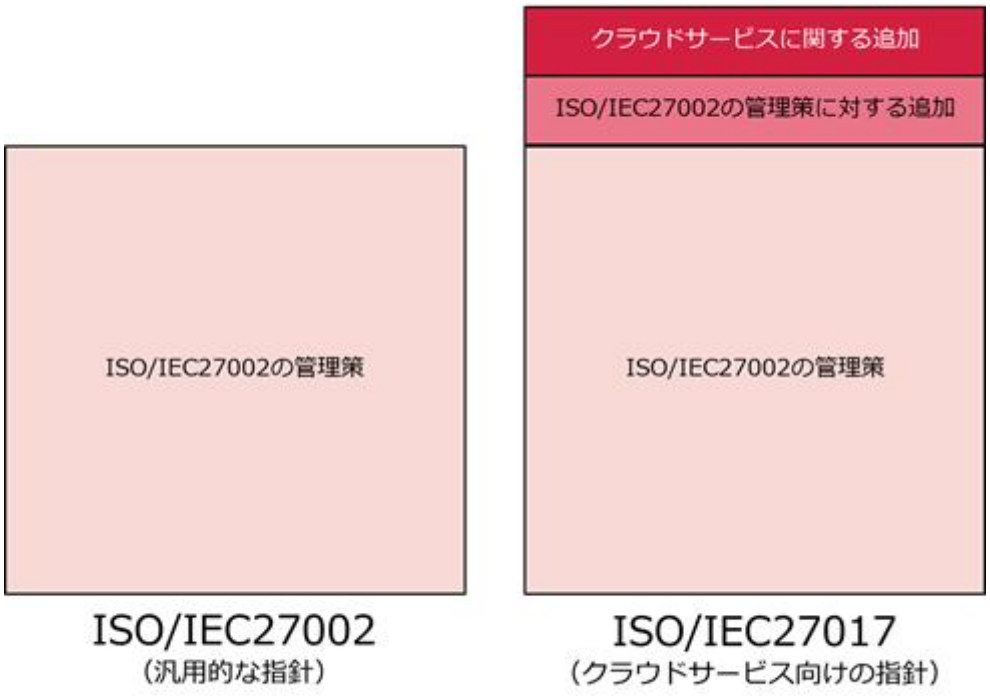


図2. ISO/IEC27002 とISO/IEC27017の体系イメージ

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 DDoS プロテクションサービスでの取り組みを次ページ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 DDoS プロテクションサービスでは、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、情報セキュリティ基本方針(http://www.iij.ad.jp/securitypolicy/index.html)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・論理的分離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を制限する

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及び責任

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。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。お客様データ（設定データ、ネットワーク情報、経路設定等）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 DDoS プロテクション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が、通信制御のための IP アドレス情報は当社バックボーン内の海外設備において一時的に保存されることがあります。

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「マニュアル」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及び責任”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ための情報は、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

契約いただ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、ご契約いただきましたサービスは、サービスコードにて、お客様毎の識別及び利用サービス、オプション機能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、サービスコード毎にラベルをつけることが可能となっております。

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 DDoS プロテクションサービス解約時並びにオプション機能解約時には、弊社サービス設備に残存したお客様の情報資産は消去いたしますが、以下のデータについては消去を実施していません。残存データへのアクセスは本サービスの運用者およびメンテナンス者に制限されており安全に管理されていますのでご安心下さい。

- 解約後も消去ができず残存するデータ
  - ✓ DDoS 対策専用ソフトウェア内データベースで管理される攻撃検知日時、検知トラフィックに対する被攻撃 IP アドレス・通信量・緩和結果
  - ✓ DDoS 対策専用ソフトウェア内データベースで版管理される保護対象 IP アドレス、攻撃検知用閾値から構成される設定情報

5. アクセス制御

5.1 利用者登録及び登録削除

ISO/IEC27017 項番：9.2.1

お客様専用のポータルサイトにて、ご契約いただ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。

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、ご契約いただ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、及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、二要素認証、及びアクセス元 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。

また、規定回数のログイン失敗によるアカウントロック機能が実装されています。

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及び利用者 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 DDoS プロテクションサービスは、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行っておりません。

5.7 仮想マシンの要塞化

ISO/IEC27017 項番：CLD9.5.2

IIJ DDoS プロテクションサービス運用ルールに基づき、IP アドレスおよびポート番号でのアクセス制御によって要塞化を行っています。

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

本サービスとの通信につきましては、お客様専用ポータルのご利用については TLS 通信にて暗号化されています。

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または再利用

ISO/IEC27017 項番：11.2.7

設備を再利用、廃棄する際には IIJ DDoS プロテクションサービス運用ルールに基づき、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

原則、サービス内容を変更する場合やメンテナンスを実施する際は、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、影響があるお客様には、お客様専用のポータルサイトに加えてあらかじめご登録いただいた運用管理登録者のメールアドレスに個別連絡いたします。

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おります。

また、お客様ご利用設備は、お客様ごとにサイジングを行っているため、契約時に保護対象における最大帯域を申告いただき適切なリソース量で提供しています。

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。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

お客様専用のポータルサイト上から以下のイベント情報を参照することが可能です。

- アノマリ検知に関する対応履歴
- アノマリ検知時のインシデントレポート
- 月次単位でのインシデントレポート

インシデントレポートの掲載期間は当日を含む 90 日間、月次報告書の掲載は過去 1 年間分となっております。

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アノマリ検知・収束時刻、対応履歴、およびそのインシデントレポートは、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 DDoS プロテクション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

弊社管理範囲のネットワークのトラフィック及び、CPU、メモリ、ディスクの使用率に関する監視は弊社が行っております。お客様毎にリソースを割り当てるシステムではないため、監視で取得した情報の提供はしておりません。

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

サービス提供システムは、オフィスネットワークとの分離を適切に行っています。

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：CLD13.1.4

お客様毎の通信経路を制御するためのネットワーク管理を適切に行っています。

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

セキュリティホワイトペーパー及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 DDoS プロテクションサービスは SaaS のクラウドサービスとなります。詳細は“IIJ DDoS プロテクションサービスのサービス概要 責任分界点”をご参照ください。

11.3 ICT サプライチェーン

ISO/IEC27017 項番：15.1.3

IIJ DDoS プロテクション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・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 IIJ DDoS プロテクションサービスと同等の情報セキュリティ水準を有していることを確認し採用しております。

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 DDoS プロテクションサービス概要 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

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いただく範囲となります。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 DDoS プロテクション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、弊社と契約者の間で訴訟の必要が生じた場合、東京地方裁判所を弊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 DDoS プロテクション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

サービス利用における対応履歴、およびインシデントレポート・ログについては、当日を含む過去 90 日分の記録を、月次報告書については過去 1 年分をお客様専用のポータルサイトにて提供しております。インシデントレポート・ログ、月次報告書については、解約日の翌々月末に全データを削除します。

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、IIJ DDoS プロテクションサービスでは、経済産業省が策定した「情報セキュリティサービス基準」への適合性を審査登録機関により審査され同基準に適合（サービス登録番号：018-

0019-40）しております。

適合サービスリスト：https://www.ipa.go.jp/security/it-service/service_list.html

IIJ DDoS プロテクションサービスの 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-YDS008-0007