セキュリティホワイトペーパー

# セキュトレ・セキュレジサービスの 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版**
**2021年10月1日**
**株式会社ワークストラスト**

# 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、株式会社ワークストラストが提供するセキュトレ、セキュレジサービス （以下、「本サービス」と表記）における ISO/IEC 27017 （以下、「ISO27017」と表記）への取り組みを解説します。
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いただき、本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情報セキュリティ向上のお役に立ちたいと考えています。

# サービス概要

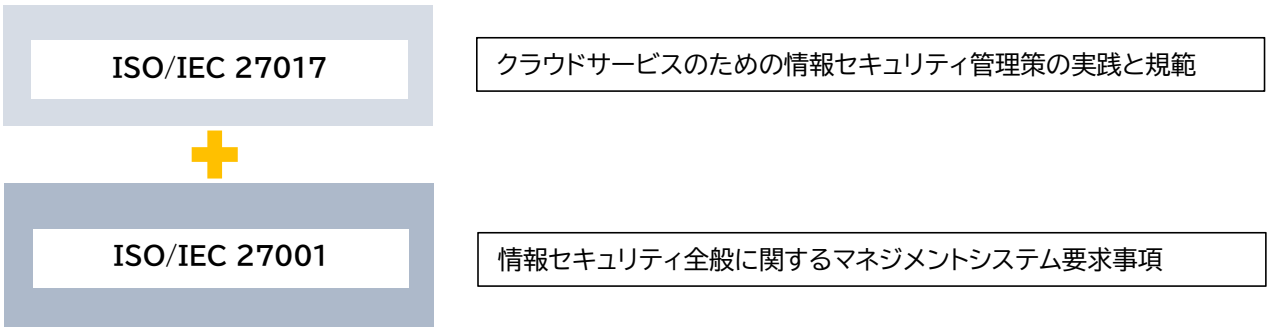
本サービスは、お客様がeラーニング、点検が行えるサービスです。
概要は https://www.security-training.jp/ をご覧ください。

本サービスは、お客様からのお申込みに基づき役務提供しています。

サービスのご利用にあたっての操作方法等につきましては、お申込みいただきましたご登録者への個別メールにてご案内いたしております（以下、「個別メール」と表記）。

# ISO27017 の概要

ISO27017は、クラウドサービスに関する情報セキュリティ管理策のガイドライン規格です。
情報セキュリティ全般に関するマネジメントシステム規格であるISO27001の取り組みをISO27017で強化することで、クラウドサービスにも対応した情報セキュリティ管理体制を構築することができます。



# ISO27017に対する取り組み

## 1. 情報セキュリティのための方針群

### 情報セキュリティのための方針群 （ISO27017 項番:5.1.1）

本サービスでは、弊社の情報セキュリティ方針に従い、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。
弊社の情報セキュリティ方針は
https://www.workstrust.com/company/policy_isms.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。

- クラウドサービスの設計及び実装に適用する最低限の情報セキュリティ要求事項
- 認可された内部関係者からのリスク
- マルチテナンシ及びクラウドサービスカスタマの隔離
- クラウドサービスプロバイダの担当職員によるクラウドサービスカスタマの資産へのアクセス
- アクセス制御手順
- 変更管理におけるクラウドサービスカスタマへの通知
- 仮想化セキュリティ
- クラウドサービスカスタマデータへのアクセス及び保護
- クラウドサービスカスタマのアカウントのライフサイクル管理
- 違反の通知、並びに調査及びフォレンジック(forensics)を支援するための情報共有指針
- バックアップの保存場所

## 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 （ISO27017 項番:6.1.1）

サービス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います。
受講者記録管理はお客様責任範囲となります。
また、本サービスは、株式会社パイプドビッツが提供しているスパイラル （ https://www.pi-pe.co.jp/spiral-series/spiral-suite/ ）を基に構築しており、システム基盤の仕様、運用はスパイラルに依存されるため、パイプドビッツ社によるスパイラルの保守、点検、整備、改良、拡張作業、中断または、セキュリティ上のリスク、脅威が生じた場合、サービスに影響がある場合があります。

### 2.2 関係当局との連絡 （ISO27017 項番:6.1.3）

弊社の本社所在地は、東京都千代田区神田駿河台3-1-7 烏山御茶ノ水ビルとなります。お問い合わせ窓口は個別メールに記載しています。なお、本サービス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（ISO27017 項番:CLD.6.3.1）
個別メールにてサービス内容を明示し、サービス提供を実施しています。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（ISO27017 項番:7.2.2）
弊社では情報セキュリティ方針（https://www.workstrust.com/company/policy_isms.html ）を定め、方針に従いサービスを運営しています。また、クラウドサービスカスタマデータ及びクラウドサービス派生データを取り扱う社員に対する定期的な教育を実施しています。

## 4. 資産の管理

### 4.1 資産目録（ISO27017 項番:8.1.1）
お客様の受講記録と弊社がサービスを運営する為の情報は、明確に分離しています。

### 4.2 クラウドサービスカスタマの資産の除去（ISO27017 項番:CLD8.1.5）
サービス解約の際、サービス解除翌日に全データを自動消去しています。

### 4.3 情報のラベル付け（ISO27017 項番:8.2.2）
お客様の受講者記録は、お客様専用の管理画面にて閲覧およびダウンロードができます。

## 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（ISO27017 項番:9.2.1）
お客様専用の管理画面にて、お申込み頂きました担当者の登録、変更、削除機能を提供しています。
登録、変更、削除に必要な手順、情報は個別メールに記載しています。

### 5.2 利用者アクセスの提供（ISO27017 項番:9.2.2）
お客様専用の管理画面は、お申込み受理後に発行された申込ID及び登録者自身が設定したパスワードでアクセスができます。

### 5.3 特権的アクセス権の管理（ISO27017 項番:9.2.3）
お客様専用の管理画面は、登録者のみが知りえる申込ID及び登録者自身が設定したパスワードでアクセスができます。

### 5.4 利用者の秘密認証情報の管理（ISO27017 項番:9.2.4）
お客様専用の管理画面を利用される際のパスワード登録、変更、再発行方法につきましては、

個別メールに記載しています。

### 5.5 情報へのアクセス制限（ISO27017 項番:9.4.1）
お客様専用のアクセス情報は、個別メールに記載しています。

### 5.6 特権的なユーティリティプログラムの使用（ISO27017 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（ISO27017 項番:CLD.9.5.1）
システム内のデータはお客様毎に論理的に分離し、制御しています。

### 5.8 仮想マシンの要塞化（ISO27017 項番:CLD 9.5.2）
不要なポートは閉じ、常駐プログラムは停止しています。

## 6. 暗号

### 6.1 暗号による管理策の利用方針（ISO27017 項番:10.1.1）
登録者の個人情報や受講者記録のデータはSSL暗号化通信によりサーバーまで伝送されています。

## 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又は再利用（ISO27017 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、資源の削除や設備の破壊を実施しています。

## 8. 運用のセキュリティ

### 8.1 変更管理（ISO27017 項番:12.1.2）
システム変更及びアップデートを実施する際は、作業内容や予定日などの情報を登録者にメールで一斉通知します。

### 8.2 容量・能力の管理（ISO27017 項番:12.1.3）
ソースの利用状況を管理し、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。

### 8.3 実務管理者の運用のセキュリティ（ISO27017 項番:CLD 12.1.5）
サービスの操作手順は、個別メールにてご案内しています。

### 8.4 情報のバックアップ（ISO27017 項番:12.3.1）
お客様専用の管理画面から受講者記録がダウンロードできますが、定期的にバックアップする

機能は付帯していません。

### 8.5 イベントログの取得（ISO27017 項番:12.4.1）
お客様の求めに応じて、ログを提供することができます。

### 8.6 クロックの同期（ISO27017 項番:12.4.4）
システムはNTPによる時刻同期を行っており、日本時間(JST)で管理しています。本サービスで記録される時刻は、すべて時刻同期に基づいて記録しています。

### 8.6 クラウドサービスの監視（ISO27017 項番:CLD 12.4.5）
本サービスに障害が有る場合、その旨がアクセスした画面に表示されます。

### 8.7 技術的ぜい弱性の管理（ISO27017 項番:12.6.1）
本サービスに影響がある技術的ぜい弱性に関する情報は、登録者にメールで一斉通知します。

## 9.通信のセキュリティ

### 9.1 ネットワークの分離（ISO27017 項番:13.1.3）
登録者および受講者のアクセスできる領域（URL)はお客様毎ユニーク（他と重複のない）なものとしており、
他のお客様と論理的に分離しています。

## 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（ISO27017 項番:14.1.1）
情報セキュリティ方針、ホワイトペーパーおよび個別メールに定めています。

### 10.2 情報セキュリティに配慮した開発のための方針（ISO27017 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・運営を実施しています。
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います。

## 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（ISO27017 項番:15.1.2）
本サービスはクラウドサービスとなり、責任分界点は、“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います。

### 11.2 ICT サプライチェーン（ISO27017 項番:15.1.3）

本サービスは、株式会社パイプドビッツが提供しているスパイラル（https://www.pi-pe.co.jp/spiral-series/spiral-suite/ ）を基に構築しています。
なお、株式会社パイプドビッツは、情報セキュリティの取り組みとしてISMSやプライバシーマークを取得していることから、一定のリスク管理、対策を実施していると思われます。（2021年10月時点）

## 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（ISO27017 項番:16.1.1）

弊社の責任範囲である、登録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、お客様専用の管理画面やメールにて速やかに報告します。

### 12.2 情報セキュリティ事象の報告（ISO27017 項番:16.1.2）

情報セキュリティ事故が発生した場合には、お客様専用の管理画面やメール等にて速やかに報告します。
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います。

## 13. 順守

### 13.1 適用法令及び契約上の要求事項の特定（ISO27017 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います。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、東京簡易裁判所または東京地方裁判所を第一審の専属的合意管轄裁判所となります。

### 13.2 知的財産権（ISO27017 項番:18.1.2）

本サービスお問い合わせ窓口はお客様への個別メールに記載しています。

### 13.3 記録の保護（ISO27017 項番:18.1.3）

お客様専用の管理画面からダウンロード可能な受講者記録は、利用期限又は解除されるまで保管しています。

### 13.4 暗号化機能に対する規制（ISO27017 項番:18.1.5）

お客様専用の管理画面および受講画面では 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（ISO27017 項番:18.2.1）

組織的な取り組みとして弊社では ISMSとプライバシーマークを取得しています。

## 改訂履歴

| 版数 | 制定/改定日 | 改定箇所、改訂理由 | 備考 |
|---|---|---|---|
| 1.0 | 2021/10/1 | 初版制定 | |