現場クラウドOne

ホワイトペーパー

株式会社 現場サポート

2026年3月1日発行 第1版

1. ホワイトペーパーの目的

『現場クラウドOneホワイトペーパー』(以下「本書」といいます)は、株式会社現場サポート(以下「当社」といいます)が商標登録し、かつ保有・運用する情報共有システム『現場クラウド One』(以下「本システム」といいます)におけるクラウドセキュリティの国際規格(ISO/IEC 27017 : 2015)で求められる要求事項の中で、当社がお客様に対し提供しているセキュリティの取組みについて明確にし、ご確認いただくことを目的としています。
ISO/IEC 27017 は、クラウドサービスの提供及び利用に適用できる情報セキュリティ管理策のための指針を示した国際規格です。
クラウドサービスに関する情報セキュリティ管理策の実践の規範として、ISO/IEC 27017によって、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ISO/IEC 27001 の取り組みを強化します。これにより、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し、その実践を支援します。

1.1. 本書の適用範囲

当社のISO/IEC 27017の適用範囲は、以下に記載しますサービス内容に対するものです。
・情報共有システム『現場クラウド One』を利用して提供する各サービス。
なお、本システムのサービスならびに各種機能については、コーポレートサイト及び製品サイトをご確認ください。

2. 当社が提供するクラウドサービス

2.1. 現場クラウドOneについて

『現場クラウド One』は、工事・業務における発注者と受注者のやりとりを円滑にする建設業専用の受発注者間情報共有システム(ASP)です。必要な書類や写真、スケジュールを簡単に共有できるほか、やりとりを文章で残しておけるので、発注者と受注者の間の連絡事項を、さらに確実で信頼性の高いものにすることができます。

3. JIS Q 27017 : 2016 (ISO/IEC 27017 : 2015) への対応

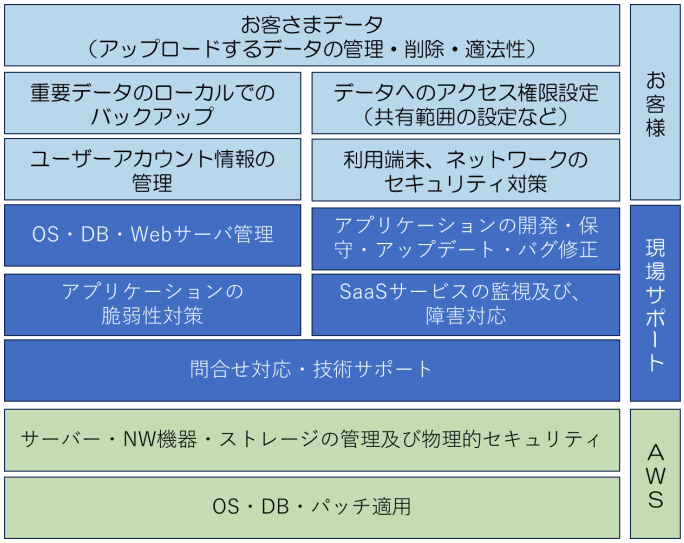
ISO/IEC 27017:2015が求める要求事項に対する当社の管理策を以下に記載します。
次項番以降はISO/IEC 27017:2015が求める要求事項に対する管理策を記載するため項番を
ISO/IEC 27017:2015に合わせて記載します。

1. 情報セキュリティのための方針群(ISO/IEC 27017:5.1.1)

当社は情報セキュリティポリシー並びにクラウドサービス情報セキュリティ方針に従いサービスを運用しています。

2. 情報セキュリティの役割及び責任(ISO/IEC 27017:6.1.1)

本システムにおける各サービス利用時の責任分界点を下図に示します。



3. 関係当局との連絡(ISO/IEC 27017:6.1.3)

- 本サービスのデータセンター所在地:日本国内(住所非公開)
- 当社(株式会社現場サポート)所在地 :鹿児島県 鹿児島市 武 1丁目 35-4

- 本サービスの開発・保守・運用および提供エリア：日本国内

重大なセキュリティに関する事象が発生した場合は、すみやかに日本国内のお客様・取引先・関係機関（個人情報保護委員会、JIPDEC、ISO27001審査機関等を含む）へ通知します。

4. 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：CLD.6.3.1）

本システムにおける各サービス利用時の責任分界点に関しては「2.情報セキュリティの役割及び責任」をご参照ください。

5. 情報セキュリティの意識向上、教育及び訓練（ISO/IEC 27017：7.2.2）

情報セキュリティ要件の周知徹底とクラウドサービスの運営ルール徹底を目的として、サービスに従事する要員を対象とした教育・訓練及び意識向上の策を実施しています。

6. クラウドサービス利用者の資産の削除（ISO/IEC 27017：CLD.8.1.5）

お客様が本サービスの個別利用（「利用規約」を参照）を終了した場合もしくは本サービスの個別利用期間（「利用規約」を参照）が終了した場合、利用規約に則りお客様が本システムに登録した情報はシステム上から削除され、該当する案件はご利用いただけなくなります。
ログおよびバックアップについての詳細は、別途当社のサービスレベル表をご確認ください。

7. 情報のラベル付け（ISO/IEC 27017：8.2.2）

本サービスでは発議文書単位で件名やタイトルの設定、重要度のラベル付けが可能となっています。

8. 利用者登録及び登録削除（ISO/IEC 27017：9.2.1）

利用者登録及び登録削除は、お客様の操作によって、利用者の登録・更新・削除を行っていただきます。

9. 利用者アクセスの提供(provisioning)（ISO/IEC 27017：9.2.2）

本サービスを利用いただく際には、利用者種別等に応じた利用者アクセス権の設定ができるようなっています。

10. 特権的アクセス権の管理（ISO/IEC 27017：9.2.3）

本システムには特権的アクセス権を有する利用者は存在しません。

11. 利用者の秘密認証情報の管理（ISO/IEC 27017：9.2.4）

利用者招待権限を有する利用者より、本サービス利用者のログインID（メールアドレス）にて招待され、招待された利用者は自らパスワードを登録いただきます。パスワード変更方法は、サポートサイトをご参照ください。

12. 情報へのアクセス制限（ISO/IEC 27017：9.4.1）

本サービスのご利用にあたっては、お客様で、お申込みいただいた利用者の利用者種別に応じて情報へのアクセス制限を行うことができます。

13. 特権的なユーティリティプログラムの使用（ISO/IEC 27017：9.4.4）

当社においては、サービス提供に必要な特権的なユーティリティプログラムについては現在使用しておりません。もし使用することになった場合は、利用者を厳しく制限し、利用の妥当性を事前に確認し、ログを取得し、レビューを実施いたします。

14. 仮想コンピューティング環境における分離（ISO/IEC 27017：CLD.9.5.1）

マルチテナント環境で動作します。テナント毎のIDによってアクセス資源を分離し、別テナントへのアクセス制御を実施しています。

15. 仮想マシンの要塞化（ISO/IEC 27017：CLD.9.5.2）

構築するすべての仮想化環境はポート・プロトコルへの制限を実施し、不正アクセスを遮断して適切にログを保存しています。

16. 暗号による管理策の利用方針（ISO/IEC 27017：10.1.1）

本サービス利用者のアカウント情報のデータベースは暗号化を行っております。
本システムにおいてお客様データをやり取りする通信はSSL/TLS（TLS 1.2/ TLS 1.3対応）通信を用いて暗号化しています。
詳細は、別途当社のサービスレベル表をご確認ください。

17. 装置のセキュリティを保った処分又は再利用（ISO/IEC 27017：11.2.7）

老朽化、故障等により交換した機器媒体の処理については、記憶媒体の物理的破壊を当社内で実施し、その後廃棄を行っています。破棄する際は専門業者へ依頼し、廃棄証明を取得しています。
機器を再利用する際はNIST 800-88以上の再生できない方法で消去し、そのあと再利用を行います。
＊「NIST SP800-88 Rev.1」はNISTが発行したIT機器のデータ消去に関するガイドラインで、現在の国際的な標準とされ、総務省は「地方公共団体における情報セキュリティポリシーに関するガイドライン」において、この規格に準拠してIT機器を処理するよう指示しています。

18. 変更管理（ISO/IEC 27017：12.1.2）

提供するサービス内容の更新や定期メンテナンスを実施する場合、当社Webサイト及び本システムのコーポレートサイトにてお知らせとして事前に通知いたします。

19. 容量・能力の管理（ISO/IEC 27017：12.1.3）

安定的なサービス提供を行うため、各サーバのリソースを監視し、必要に応じてキャパシティの増強を行っています。

20. 実務管理者の運用のセキュリティ（ISO/IEC 27017：CLD.12.1.5）

本システムの操作方法は、本サービスのサポートサイトにて提供しています。

21. 情報のバックアップ（ISO/IEC 27017：CLD.12.3.1）

本システムのバックアップは、お客様の情報資産を含む各種登録ファイルについては1回/日、データベースについては1回以上/日で実施しています。
バックアップデータは暗号化を行い保管しています。「16.暗号による管理策の利用方針」に記載の通りです。
詳細は、別途当社のサービスレベル表をご確認ください。

当社がシステムの運営、維持のため実施するバックアップの内容は以下の通りです。

- バックアップ
    - データストレージは日次で別ストレージにバックアップを保管し、データベースはストレージバックアップとは独立して別途バックアップを取得して別ストレージに保管します。
    - ハードウェアの障害が複数個所で同時に起きるなど、予測し得ない多重的な機器障害が発生した場合、システムにご登録いただいたデータの一部を復元できない可能性があります。不可抗力な機器障害に基づく登録データの喪失につきましては、当社では責任を負うことができません。予めご了承下さい。

- お客様の登録データのバックアップは10世代、データベースのバックアップは10日間保持し、この期間が経過しましたら削除いたします。

- 事業継続戦略等
  - 当社の瑕疵によるシステム障害が発生した場合のデータ復旧時点目標（RPO）は、標準復旧時点目標を障害が起こる直前のデータとし、最低復旧時点目標を障害時点前の最新のバックアップデータ（最大24時間）とします。

- 登録情報のシステム内保持期間
  - 本サービスの個別利用に係わるデータは、個別利用開始日からその利用を終了させる操作（工事完了等）が発生するまでを保持期間とします。
  - 個別利用を終了させる操作（工事完了等）が発生しなかった場合は、個別利用期間を経過した時点で、システムから対象案件に係わるデータのみを消去します。
  - 企業、利用者等の各情報につきましては、上記の限りではありません。削除を希望される場合は、サポート窓口までご連絡下さい。

22. イベントログ取得（ISO/IEC 27017：CLD.12.4.1）

本システムの維持管理に必要となる適切なログを取得しています。重要なインシデントが発生し、実態調査を目的としたログ情報等が必要な場合または所定の手順でログの提示を求められた場合、有償により開示できる範囲で利用者に提供することができます。
また、重要なインシデントが発生し、実態調査を目的としたログ情報等が必要な場合には、お申し出のあった後に社内協議を行い必要に応じて対応いたします。
ログについては、別途当社のサービスレベル表をご確認ください。

23. クロックの同期（ISO/IEC 27017：CLD.12.4.4）

本システムではNTP サーバを参照することで時刻を同期（日本標準時）しています。

24. クラウドサービスの監視（ISO/IEC 27017：CLD.12.4.5）

クラウドプロバイダの監視機構を用いることで、不正に利用されていないことを常に監視しています。また、CPU・メモリ・ディスクの使用率等のシステムに関するリソース状況も監視しています。

25. 技術的ぜい弱性の管理（ISO/IEC 27017：12.6.1）

定期的にぜい弱性情報の収集を実施し、当社の責任の範囲で対応が必要となった場合には、定期または緊急メンテナンスにて対応を実施します。
メンテナンス情報は当社コーポレートサイト及び本サービスのサポートサイトにて、お知らせとして通知いたします。

26. ネットワークの分離（ISO/IEC 27017：13.1.3）

当社の社内ネットワークと本システムのネットワークは物理的に分離しています。

27. 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/IEC 27017：CLD.13.1.4）

物理ネットワークと論理ネットワークの整合性がとれるように設計、構築、管理を徹底しています。

28. 情報セキュリティ要求事項の分析及び仕様化（ISO/IEC 27017：14.1.1）

当社では、情報セキュリティ方針の下で、お客様が要求される情報セキュリティを維持、提供しています。
主にお客様が検討される情報セキュリティの機能の仕様として、本書は以下の項目を記載しています。

- アクセス制限機能（12. 情報へのアクセス制限、15. 仮想マシンの要塞化）
- 通信暗号化機能（16. 暗号による管理策の利用方針）
- バックアップ機能（21. 情報のバックアップ）

- ログ取得機能（22. イベントログ取得）

詳細は、別途当社のサービスレベル表をご確認ください。

29. セキュリティに配慮した開発のための方針（ISO/IEC 27017：14.2.1）

当社では、システムを開発する際は、プロジェクト毎のタスク管理にて、セキュリティに配慮したコーディングによって不正アクセスやマルウェアの感染を防止するなど、セキュリティに十分配慮した開発を行っています。

30. 供給者との合意におけるセキュリティの取扱い（ISO/IEC 27017：15.1.2）

当社とお客様の責任分界点や当社のセキュリティ対策は、本書・利用規約に記載しております。
お客様にはこれらにご同意いただいた上で本サービスをご利用いただいております。
本システムにおけるサービス利用時の責任分界点に関しては「2.情報セキュリティの役割及び責任」をご参照ください。

31. ICTサプライチェーン（ISO/IEC 27017：15.1.3）

当社が利用するクラウドサービスプロバイダの情報セキュリティ水準を把握し、本システムの情報セキュリティとの整合性が取れていることを確認しています。

32. 責任及び手順（ISO/IEC 27017：16.1.1）

利用者に大きな影響を与えるセキュリティインシデント（データの消失、長時間のシステム停止等）が発生した場合は、当社コーポレートサイトにて通知いたします。
セキュリティインシデントに関するお問合せは、当社サポートセンターより受け付けています。
サービスレベルについての詳細は別途当社のサービスレベル表をご確認ください。

33. 情報セキュリティ事象の報告（ISO/IEC 27017：16.1.2）

当社コーポレートサイト及び本サービスのサポートサイトにてお知らせとして通知いたします。
また個別のお問い合わせは、当社サポートセンターにより受付けています。

34. 証拠の収集（ISO/IEC 27017：16.1.7）

裁判所からの開示請求など、法律に基づいた正当な開示請求が行われた場合、お客様の同意なく、お客様のデータを当該機関に開示することがあります。詳細は、本システムの利用規約をご確認ください。なお、お客様に重要なインシデントが発生し、実態調査を目的としたログ情報等が必要な場合には当社サポートセンターまでお問い合わせください。
ログについては、別途当社のサービスレベル表をご確認ください。

35. 適用法令及び契約上の要求事項の特定（ISO/IEC 27017：18.1.1）

本システムの利用に関して、適用される「準拠法」は「日本法」となります。
本システムの運用に関連する各種法令に関しては『法令及びその他規範一覧』に登録し、法的準拠するように努めています。

36. 知的財産権（ISO/IEC 27017：18.1.2）

本サービスをご利用いただく上で知的財産権に関わるお問い合わせは、当社サポートセンターまでお問い合わせください。

37. 記録の保護（ISO/IEC 27017：18.1.3）

当社は、本システムに関する利用記録に対して、不正アクセス・改ざんなどを防ぐためアクセス制限を実施しています。
利用記録の記録期間や保存期間については、別途当社のサービスレベル表をご確認ください。

38. 暗号化機能に対する規制（ISO/IEC 27017：18.1.5）

本システムのソフトウエア、及び装置等を、海外に持ち出すことはありません。従って、暗号化機能については、日本国内法に準拠します。

39. 情報セキュリティの独立したレビュー（ISO/IEC 27017：18.2.1）

当社では、内部監査、マネジメントレビュー、定期のリスクアセスメントの実施に加え、以下の第三者による認証審査を受けて情報セキュリティに対する取り組みを行うことで、安全なセキュリティレベルを確保します。

【サービスレベル表】

サービス基本特性			
品質サービス			
項目	内容	当社対策	当社備考
サービス稼働設定値	サービス提供時間・サービス稼動時間・稼働率の現状または最低限達成しようとしている目標値	99.5%以上	
認証取得、監査実施	プライバシーマーク、ISMS、ITSMSの取得、18号監査の監査報告書作成の認証名・監査名	【当社】 プライバシーマーク、ISMS 【データセンター】 プライバシーマーク、ISMS	Uptime Institute TierIII
アプリケーション・基盤・ストレージ			
セキュリティ			
記録（ログ等）	a）利用者の利用状況の記録（ログ等）の保存期間	1年	
	b）例外処理の記録（ログ等）の保存期間	1年	
	c）情報セキュリティ事象の記録（ログ等）の保存期間	1年	
	d）ログの削除	上記保存期間を過ぎたもの	
バックアップ体制	バックアップ場所及びバックアップ媒体	場所：データセンターメディア：別ストレージサーバ	
	自動バックアップ	1回/日：登録ファイル1回以上/日：データベース	登録ファイル： 添付文書等 データベース： 承諾情報等
	バックアップの削除	「21.情報のバックアップ」に記載	
ネットワーク			
回線			
ネットワーク監視	サービスへのネットワークアクセスにおいて障害が発生した際の通報時間	検知後60分	ポータルサイト及び当社Webサイトでのご案内
ファイアフォール	不正アクセスやサイバー攻撃からネットワークやデータの保護	設定済み	
なりすまし対策	第三者によるサーバなりすましに関する対策の実施	あり	メンテナンス接続IP制限、鍵認証等
通信の暗号化	データの暗号化	あり	TLS1.2以上可 （TLS1.0、SSL不可）
サービスサポート			
サービス窓口			
障害対応	システムの復旧速度	48時間以内に95%	
	インシデントが発覚してから通知を行うまでの目標時間	24時間	
サポート体制（操作マニュアル等）	利用時のサポート体制	ポータルサイトの運用、操作マニュアル、ヘルプデスク	ポータルサイトで案内
サポート体制（操作説明会等）	操作説明会の開催支援	操作説明会の開催	当社Webサイトで案内