情報セキュリティホワイトペーパー

当ホワイトペーパーは、CCJ株式会社（以下、「当社」）が提供するクラウドサービスである Sustaina Cloud（以下、「本サービス」）に関する情報セキュリティへの取り組みを記載したものです。記載内容については、クラウドサービスに関する情報セキュリティの国際規格である ISO/IEC 27017:2015 において、クラウドサービス事業者が、クラウドサービス利用者に対して、開示もしくは公開を求めている事項に基づき構成されています。なお、各項目の末尾に記載されているカッコは、ISO/IEC 27017:2015 の該当する項番を表しています。

1. Sustaina Cloudについて

1.1. Sustaina Cloud（サステナクラウド）は、サスティナビリティ情報開示およびサスティナビリティ関連業務を支援することを目的としたSaaS（Software as a Service）です。本サービスを構成するインフラストラクチャーは、Amazon Web Services Inc.が提供する、AWS（Amazon Web Services）を採用しています。

2. 情報セキュリティのための方針群

2.1. 本サービスは、当社の定めた情報セキュリティ基本方針に従い、サービス運営を行います。詳細は、クラウドセキュリティ基本方針をご覧ください。

（ISO/IEC 27017:2015 5.1.1 CSP）

3. 情報セキュリティの役割および責任

3.1. 本サービス の利用においては、お客様と当社の間でセキュリティ対策に関する責任分担が求められます。以下は、本サービスに関する責任分界点です。

内容	責任範囲
保存されたデータおよびアカウント情報	お客様
エンドポイントのセキュリティ	
情報セキュリティ対策	当社
データの保護	
アプリケーション	
ミドルウェア	
OS	
コンテナ	

（ISO/IEC 27017:2015 6.1.1 CSP）

4. 関係当局との連絡

4.1. 当社の所在地は、ホームページ（https://creative-capitalism.co.jp/）でご確認ください。お客様からお預かりしたデータは、AWS東京リージョンに保管しています。

（ISO/IEC 27017:2015 6.1.3 CSP）

5. クラウドコンピューティング環境における役割および責任の共有および分担

5.1. 責任分界点の詳細に関しては前出の「2. 情報セキュリティの役割および責任」をご参照ください。

（ISO/IEC 27017:2015 CLD 6.3.1 CSP）

6. 情報セキュリティの意識向上、教育及び訓練

6.1. 情報セキュリティの確保と重要性を認識する為に、必要な教育・訓練を定期的に実施しています。

（ISO/IEC 27017:2015 7.2.2 CSP）

7. 資産目録

7.1. お客様が保存したデータと、当社がサービスを運営するための情報は明確に分離しています。

（ISO/IEC 27017:2015 8.1.1 CSP）

8. クラウドサービスカスタマの資産の除去

8.1. 利用契約の終了後、当社の運用上合理的な期間内に、お客様が作成・保存したデータおよびバックアップデータは完全に削除します。

8.2. 本サービスでは、お客様が作成・保存したデータをエクスポートできる機能を提供しています。

8.3. 但し、お客様のデータを含まない本サービスの運用に関するログは対象外とします。

（ISO/IEC 27017:2015 CLD 8.1.5 CSP）

9. 情報のラベル付け

9.1. お客様が作成したデータ項目およびアンケートの質問にはラベルをつけることができ、情報の分類を行うことが可能です。

（ISO/IEC 27017:2015 8.2.2 CSP）

10. 利用者登録及び登録削除

10.1. ユーザーアカウントの登録および削除は、サービス内で行っていただくことが可能です。

10.2. 初期パスワードは、アカウントの登録時に届くメールに記載されたリンクをクリックすることで、お客様自らが設定いただけます。

10.3. 提供機能の利用にあたっては、サービスヘルプページの操作マニュアルをご参照ください。

（ISO/IEC 27017:2015 9.2.1 CSP）

11. 利用者アクセスの提供

11.1. お客様は、お客様が追加したユーザーを管理者、一般、閲覧者の3つの権限に分類することが可能です。各権限における機能は以下の通りです。

権限	機能
管理者	全てのデータを閲覧、操作、編集することが可能です。
一般	管理者からアサインされたタスクの情報のみ閲覧、操作、編集することが可能です。
閲覧者	全てのデータを閲覧することが可能です。操作や編集はできません。

（ISO/IEC 27017:2015 9.2.1 CSP, 9.2.2 CSP, 9.2.2 CSP）

11.2. 提供機能の利用にあたっては、サービスヘルプページの操作マニュアルをご参照ください。

12. 特権的アクセス権の管理

12.1. 本サービスをご利用する際にはご登録いただいたメールアドレスとパスワードを入力し認証していただく必要があります。

12.2. 設定できるパスワードは 12 文字以上で、アルファベット、数字、記号が設定できます。アルファベットについては大文字と小文字は区別されます。

12.3. 現在、多要素認証によるログイン機能は提供しておりません。

（ISO/IEC 27017:2015 9.2.3 CSP）

13. 利用者の秘密認証情報の管理

13.1. 本サービス開始時に、代表のお客様へ初回ログイン手順をメールにて提供します。

13.2. パスワードの変更やリセットが可能です。サービスヘルプページの操作マニュアルをご参照ください。

（ISO/IEC 27017:2015 9.2.4 CSP）

14. 情報へのアクセス制限

14.1. 「11. 利用者アクセスの提供」で示した通り、管理者権限を有するお客様によってユーザーの権限の分類およびユーザーの追加・削除を行うことができます。

（ISO/IEC 27017:2015 9.4.1 CSP）

15. 特権的なユーティリティプログラムの使用

15.1. 本サービスにおいて、通常の操作手順またはセキュリティ手順を回避することのできるユーティリティプログラムの提供はありません。

（ISO/IEC 27017:2015 9.4.4 CSP）

16. 仮想コンピューティング環境における分離

16.1. 本サービスでは、データベースおよびストレージをお客様ごとに論理的に分離しています。

（ISO/IEC 27017:2015 CLD 9.5.1 CSP）

17. 仮想マシンの要塞化

17.1. お客様が利用する仮想環境は、IPアドレスによるアクセス制限やポート制限など、各種のセキュリティ機能を有効化しています。

（ISO/IEC 27017:2015 CLD 9.5.2 CSP）

18. 暗号による管理策の利用方針

18.1. お客様の情報を保存するためのデータベースとして利用しているAmazon RDSはAES-256暗号化アルゴリズムを使用し暗号化されています。

18.2. 本サービスにおける通信は全てSSL/TLS 通信によって暗号化されています。

（ISO/IEC 27017:2015 10.1.1 CSP）

19. 装置のセキュリティを保った処分または再利用

19.1. 物理装置の資産はありませんが、AWS内で利用されたストレージデバイスなどの装置の処分に関してはAWSの廃棄プロセスであるNIST 800-88に詳細が説明されている方法を使用してメディアを廃棄しています。

（ISO/IEC 27017:2015 11.2.7 CSP）

20. 変更管理

20.1. 本サービスに影響のある変更およびメンテナンスを実施する場合には、事前にメールにて通知を行います。また、本サービスの仕様変更について利用規約に定め、サービスを提供します。

（ISO/IEC 27017:2015 12.1.2 CSP）

21. 容量・能力の管理

21.1. リソース等のメトリクスに対して日々の稼働監視を行っています。

（ISO/IEC 27017:2015 12.1.3 CSP）

22. 実務管理者の運用のセキュリティ

22.1. ご契約いただいたお客様に対し、本サービスの利用に必要な操作マニュアルを提供しています。

（ISO/IEC 27017:2015 CLD 12.1.5 CSP）

23. 情報のバックアップ

23.1. 本サービスでは、全てのお客様のデータを日次で取得し、バックアップは7日間保管されます。

（ISO/IEC 27017:2015 12.3.1 CSP）

24. イベントログ取得

24.1. 本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。また、管理者権限を有しているお客様へは、ユーザーが行った特定機能に対する操作ログを本サービス上で確認することが可能です。

（ISO/IEC 27017:2015 12.4.1 CSP）

25. 実務管理者及び運用担当者の作業ログ

25.1. 本サービスでは、サービスの提供に関わる作業及び結果を記録し、レビューを実施しています。

（ISO/IEC 27017:2015 12.4.3 CSP）

26. クロックの同期

26.1. 本サービス内で提供されるログは、タイムゾーンJST(UTC+9)で提供されます。

26.2. ログの時刻は、AWSが提供するNTPサーバー（Amazon Time Sync Serivce）を参照し、時刻の同期を行っています。

（ISO/IEC 27017:2015 12.4.4 CSP）

27. クラウドサービスの監視

27.1. ネットワークおよび CPU・メモリ、サーバーエラー等の各メトリクスの監視は、当社が実施しています。また、管理者権限を有しているお客様へは、ユーザーが行った特定機能に対する操作ログを本サービス上で確認することが可能です。

（ISO/IEC 27017:2015 CLD 12.4.5 CSP）

28. 技術的ぜい弱性の管理

28.1. 本サービスでは、OS、ミドルウェア、フレームワークおよび利用するクラウドサービスに関する脆弱性情報を継続的に収集し、当社サービスへの影響を評価しています。

28.2. 影響があると判断された場合には、当社の責任範囲において、パッチ適用、設定変更、代替措置の実施等、適切な対応を速やかに行います。

28.3. また、開発および運用に関与する関係者に対しては、ハードウェアおよびソフトウェアの安全な取り扱いに関する情報セキュリティ対策を周知し、適切な運用が行われるよう管理しています。

28.4. これらの取り組みにより、技術的脆弱性によるリスクを低減し、サービスの安全性確保に努めています。

（ISO/IEC 27017:2015 12.6.1 CSP）

29. ネットワークの分離

29.1. お客様ごとに会社IDでユーザーテーブルを分けて管理し、ネットワークの仮想化技術を利用し他のお客様とのネットワークの分離を適切に行っています。

（ISO/IEC 27017:2015 13.1.1 CSP）

30. 仮想および物理ネットワークのセキュリティ管理の整合

30.1. 本サービスで採用しているAWSは、第三者機関の認証を多く取得し、高い信頼性を持つ仮想化サービスであることを確認しています。

（ISO/IEC 27017:2015 CLD 13.1.4 CSP）

31. 情報セキュリティ要求事項の分析および仕様化

31.1. 当社は、本サービスおよび当社が遂行する他の全てのプロジェクトに対して情報セキュ

リティ要求事項の分析を行い、プロジェクトペーパーを作成しています。

31.2. プロジェクトペーパーには、職務分掌、リスクアセスメント、リスク低減策、システムアーキテクチャーの構成から検収要件まで、セキュリティに配慮した開発ライフサイクルを構築しています。

（ISO/IEC 27017:2015 14.1.1 CSP）

32. セキュリティに配慮した開発のための方針

32.1. 本サービスは、当社の情報セキュリティ規則およびコーディング・コードレビュー規則に則った開発を実施しています。また、開発を外部に委託する際も、これに準じた契約のもと開発が行われます。

32.2. 本サービスにアップデートがあった場合は、公開前にステージング環境で網羅的なテストを実施し、品質を担保します。

（ISO/IEC 27017:2015 14.2.1 CSP）

33. 供給者との合意におけるセキュリティの取扱い

33.1. 責任分界点の詳細に関しては前出の「2. 責任分界点について」をご参照ください。

33.2. 本サービスに関係する全ての供給者に対しては、契約のもと当社の情報セキュリティ規則に従う合意を得ています。また、当社は定期的に供給者のリスクアセスメントおよびセキュリティチェックを実施しています。

（ISO/IEC 27017:2015 15.1.2 CSP）

34. ICT サプライチェーン

34.1. 当社は、本サービスの提供に際し、ピアクラウドサービスとしてAWSを採用しています。当該サービスが当社の情報セキュリティ方針を満たしていることを確認するとともに、都度必要なリスクマネジメントを実施しています。

（ISO/IEC 27017:2015 15.1.3 CSP）

35. 責任および手順

35.1. 当社が確認したセキュリティインシデントに関しては、当社の情報セキュリティインシデント対応マニュアルに則り適切に対応しています。また、確認したセキュリティインシデントがお客様に重大な影響を及ぼす場合、確認より24時間以内を目標に代表のお客様へメールにて通知を行います。

（ISO/IEC 27017:2015 16.1.1 CSP）

36. 情報セキュリティ事象の報告

36.1. 情報セキュリティインシデントの相談・報告窓口として、以下連絡先を提供しています。

36.2. 連絡先メールアドレス：info@creative-capitalism.co.jp

（ISO/IEC 27017:2015 16.1.2 CSP）

37. 証拠の収集

37.1. 本サービスは、ユーザーが行った特定機能に対する操作ログを確認できる機能を提供し

ています。当社責任範囲でのアクセスログ等のデジタル証跡が必要な場合は、お客様の要望に対して個別に対応しています。都度、当社までお問い合わせください。

37.2. 本サービスの利用規約に同意いただく際、法律や裁判所の命令によって開示が必要とされる場合、お客様に通知するか同意を得ることなく情報を開示することができることをご了承いただく必要があります。

（ISO/IEC 27017:2015 16.1.7 CSP）

38. 適用法令および契約上の要求事項の特定

38.1. 本サービスの利用に関して、適用される準拠法は日本法となります。また、当社はプライバシーマークによる認証を取得しています。

（ISO/IEC 27017:2015 18.1.1 CSP）

39. 知的財産権

39.1. 知的財産権に関わるお問い合わせは、下記の窓口へお問い合わせください。

39.2. 連絡先メールアドレス：info@creative-capitalism.co.jp

（ISO/IEC 27017:2015 18.1.2 CSP）

40. 記録の保護

40.1. 当社は、法定保管期間年数が決まっている情報やその他のログを保存期間を定め取得・保護しています。

（ISO/IEC 27017:2015 18.1.3 CSP）

41. 暗号化機能に対する規制

41.1. 本サービスはAWSが提供する標準機能を利用しAES-256 形式で暗号化を行い保管されます。輸出規制の対象となる暗号化の利用はありません。

（ISO/IEC 27017:2015 18.1.5 CSP）

42. 情報セキュリティの独立したレビュー

42.1. 当社は、ISO/IEC 27001 と ISO/IEC 27017 について第三者による審査を受けるとともに、それらに関する独立した内部監査を実施しています。

（ISO/IEC 27017:2015 18.2.1 CSP）

43. 認証

43.1. 当社は、情報マネジメントシステム認定センター(ISMS-AC)が運営する、ISMS 適合性評価制度における下記認証を取得しています。

43.2. ISMS 認証： JIS Q 27001:2014 (ISO/IEC 27001 : 2013)

43.3. ISMS クラウドセキュリティ認証： JIP-ISMS517-1.0 (ISO/IEC 27017 : 2015)