ISO/IEC 27017　ホワイトペーパー

第 1.2 版

2024 年 6 月

株式会社インフォネット

目次

1. はじめに

1.1 ホワイトペーパーの目的

「ISO/IEC 27017　ホワイトペーパー」（以下、本書）は、クラウドセキュリティの国際規格（ISO/IEC 27017）で求める要求事項に対して、クラウドサービスプロバイダ（CSP）が実施する管理策をご確認いただくことを目的としています。

1.2 本書の適用範囲

弊社の提供するコンテンツマネジメントシステム「infoCMS10」が、本書の適用範囲となります。

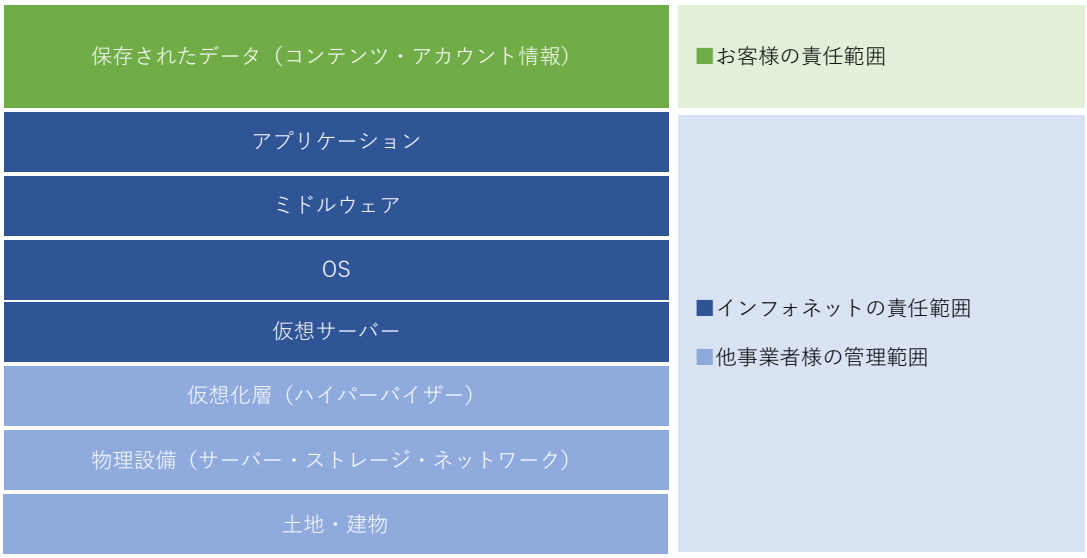
2. infoCMS について

2.1 infoCMS とは

商用 CMS としてあらゆる企業・団体様において理想的な WEB サイトの構築が可能です。
WEB 担当者の業務負担軽減と効果的な WEB マーケティングを実現する高機能・オールインワンパッケージの CMS です。

2.2 責任分界点について

infoCMS に関する責任分界点は、以下になります。



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

3.1 管理策に関する見方の説明

JIS Q 27017:2016（ISO/IEC 27017:2015）が求める要求事項に対する管理策を記載します。

番号・タイトルは ISO27017 が求める”情報セキュリティ管理策の実践の規範”箇条 5～18（17 箇条を除く）の小項番番号・要求事項原文を示し、後に続く内容は、弊社サービスの要求事項に対する解釈および管理策になります。

3.2 各管理策への対応について

ISO/IEC 27017 は、ISO/IEC27002 と共通する管理策については、同じ項番が付与されていますので、ISO/IEC27001 付属書 A の項番とも一致します。

クラウド特有の拡張された管理策については、「付属書 A（規定）クラウドサービス拡張管理集」として、頭に「CLD」がつく項番が指定されています。頭に「CLD」がつく管理策についても、そのあとに続く番号は、ISO/IEC27001 付属書 A および ISO/IEC27002 で定められた番号とも整合がとられています。

本書は、項番の順に沿ってクラウドサービスプロバイダ（CSP）としての取り組みについて解説を行います。

5.1.1 情報セキュリティのための方針群

本サービスは、弊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、情報セキュリティ基本方針（https://www.e-infonet.jp/sustainability/corporategovernance/security.html）をご覧ください。

6.1.1 情報セキュリティの役割および責任

責任分界点については「2.2 責任分界点について」で明記しています。

6.1.3 関係当局との連絡

弊社の所在地は、ホームページ（https://e-infonet.jp/）でご確認ください。

なお、弊社が提供するクラウド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。

CLD.6.3.1 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

役割および責任は「2.2 責任分界点について」に記載しています。また、本サービス利用については利用規約をご確認ください。

7.2.2 情報セキュリティの自覚、教育および訓練

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。

8.1.1　資産目録

サービス利用者様の情報資産（保存データ）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います。

CLD.8.1.5　クラウドサービスカスタマの資産の除去

本サービスの提供が終了した場合に、サービス利用者様が作成・保存した情報資産（保存データ）に関しては、削除サイクルに従って破棄するものとします。バックアップについても同様に破棄いたします。

但し、サービス利用者様の情報資産を含まないサービス共通ログは対象外とします。

8.2.2　情報のラベル付け

本サービスは、情報資産の分類（サービス利用者様にて保存されるデータ）にご利用頂けるラベル付け機能を持っています。

9.2.1　利用者登録および登録削除

本サービス開始時に管理者権限を有する利用者 ID を提供します。

提供した利用者 ID にて運営時に必要となる利用者の登録・更新・削除の機能がご利用いただけます。提供機能の利用にあたっては、操作マニュアルをご参照ください。

9.2.2　利用者アクセスの提供(provisioning)

本サービスのユーザ権限を管理する機能（アクセス権、機能制限設定等）を提供しており、管理者が設定可能となります。

提供機能の利用にあたっては、操作マニュアルをご参照ください。

9.2.3　特権的アクセス権の管理

ID／パスワード認証に加え、アクセス元 IP アドレス制限を設定できるオプションを提供しています。

9.2.4　利用者の秘密認証情報の管理

本サービス開始時に管理者権限を有する利用者 ID をメールまたは郵送にて提供します。

パスワード変更にあたっては、操作マニュアルをご参照ください。

9.4.1　情報へのアクセス制限

管理者権限を有するサービス利用者様によって機能制限を行うことができます。

9.4.4　特権的なユーティリティプログラムの使用

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。

CLD.9.5.1　仮想コンピューティング環境における分離

仮想化技術やネットワークセキュリティ技術を利用し、サーバやネットワーク、ストレージは論理的に分離し、制御しています。

CLD.9.5.2　仮想マシンの要塞化

仮想マシンの要塞化のために、IP/プロトコル/ポートへのアクセス制限などを実施しています。

10.1.1　暗号による管理策の利用方針

本サービス利用におけるデータをやり取りする通信は、 SSL/TLS 通信を行うオプションを提供しています。

11.2.7　装置のセキュリティを保った処分または再利用

故障などにより交換となった記憶媒体の処理については、弊社と機器ベンダーとの契約に基づき適切に処理を行っています。

12.1.2　変更管理

本サービスの利用者様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。

12.1.3　容量・能力の管理

弊社にて日々のプロセスの中で稼働監視を行っています。
また、本サービスの管理者向けに利用状況を確認する機能を提供しています。
契約容量の 90%を超過した際、管理者のメールアドレスに通知メールが送信される基本設定となっています。

CLD.12.1.5　実務管理者の運用のセキュリティ

本サービスでは、サービスの利用に必要な操作手順を、マニュアルなどのドキュメントとして提供しています。

12.3.1　情報のバックアップ

本サービスでは、サービスの提供に用いる仮想環境のバックアップを、日次で 3 世代を取得/保持しています。

12.4.1　イベントログ取得

弊社の責任範囲において、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。必要あればお問い合わせください。また、サービス利用者様向けにログインログを確認できる機能を提供しています。

12.4.4　クロックの同期

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。

CLD.12.4.5　クラウドサービスの監視

ネットワークおよび CPU・メモリ等の使用率増加を検知する監視は、弊社が実施しています。
監視結果が必要となる場合、弊社サポート窓口までご連絡ください。

12.6.1　技術的ぜい弱性の管理

定期的に脆弱性情報の収集を行い、お客様に影響を及ぼす、またはプロダクトのメンテナンスを必要とする情報については、弊社サポート窓口よりメールにて案内を行っています。
メンテナンスを必要とする場合は、対応前に実施日時や対応内容を連絡しています。

13.1.3　ネットワークの分離

ネットワークの仮想化技術を利用し、他のサービス利用者様とのネットワークの分離を適切に行っています。また、弊社の社内ネットワークと本サービス側のネットワークとは、物理的に分離されています。

CLD.13.1.4　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

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。

14.1.1　情報セキュリティ要求事項の分析および仕様化

本サービスの主なセキュリティ機能は以下となります。

- ウィルスチェック機能
- ログ管理機能
- 監視機能

14.2.1　セキュリティに配慮した開発のための方針

弊社のコーディング規則に則ったシステム開発を行い、第三者による定期的なセキュリティ診断を実施しています。

15.1.2　供給者との合意におけるセキュリティの取扱い

責任分界点の詳細に関しては前出の「2.2 責任分界点について」をご参照ください。
また、セキュリティ対策に関しても「2.2 責任分界点について」に記載する弊社サービスの提供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。

15.1.3　ICT サプライチェーン

本サービスの提供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、弊社セキュリティ方針を満たすようリスク管理を実施しています。

16.1.1　責任および手順

弊社で確認できたセキュリティインシデントに関しては、情報セキュリティ基本方針に則り、適切に対応しています。
また、確認できたセキュリティインシデントがサービス利用者様に重大な影響を及ぼす可能性がある場合には、対象のお客様に対し、弊社サポート窓口より通知を行います。
なお、通知手順および通知目標時間については、要件定義書をご参照ください。

16.1.2　情報セキュリティ事象の報告

情報セキュリティ事故が発生した場合には、メール等で速やかに報告いたします。
また、お問い合わせ窓口にて、メールを用い相互に情報のやりとりができる仕組みを提供しています。

16.1.7　証拠の収集

法令または裁判所の命令に基づき開示が義務付けられた際、お客様への通知または同意を経ることなく開示することついて、利用規約に合意いただく必要があります。

18.1.1　適用法令および契約上の要求事項の特定

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。

18.1.2　知的財産権

知的財産権に関わるお問い合わせは、弊社サポート窓口へお問い合わせください。

18.1.3　記録の保護

弊社の責任範囲において、保存期間を定めログを取得しています。必要な場合は、弊社サポート窓口へお問い合わせください。

18.1.5　暗号化機能に対する規制

本サービスへの Web アクセスにおいては、SSL/TLS 通信を行うオプションを提供しています。
なお、輸出規制の対象となる暗号化の利用はありません。

18.2.1　情報セキュリティの独立したレビュー

ISO/IEC 27001 および JIP-ISMS517-1.0（ISO/IEC 27017）について第三者による審査を受け、それぞれの認証を取得しております。

4. 更新履歴

版数	日付	更新内容
第 1.0 版	2022/6/1	初版公開
第 1.1 版	2023/7/1	18.2.1　ISO/IEC 27017 認証取得による表記変更
第 1.2 版	2024/6/17	5.1.1　情報セキュリティ基本方針の記載 URL 変更