# UTILIX クラウドサービス ホワイトペーパー

第 7.0 版

アズビル株式会社

グループクラウドサービス部

| 版数 | 改訂日 | 改訂理由及び内容 |
|---|---|---|
| 1.0 版 | 2020.03.02 | 初版発行 |
| 2.0 版 | 2020.03.23 | 16.1.1 責任及び手順 についてより詳細に記述 |
| 3.0 版 | 2020.04.28 | 発行部署名改訂<br>10.1.1 暗号による管理策の利用方針 を改訂<br>11.2.7 装置のセキュリティを保った処分又は再利用 を改訂<br>12.4.4 クロックの同期 を改訂<br>14.1.1 情報セキュリティ要求事項の分析及び仕様化 を改訂 |
| 4.0 版 | 2021.11.30 | 6.1.1 情報セキュリティの役割及び責任 を改訂(などを追記)<br>10.1.1 暗号による管理策の利用方針 を改訂(SSL を削除) |
| 5.0 版 | 2022.12.08 | 全般 誤記などの軽微な文言修正。<br>2.2. 当社を弊社に修正。<br>5.1.1 情報セキュリティ基本方針を情報セキュリティ方針に修正。 |
| 6.0 版 | 2023.03.03 | 目次の更新<br>azbil グループ情報セキュリティ基本方針の制定に伴う文言修正および誤記などの軽微な文言修正<br>5.1.1 azbil グループ情報セキュリティ基本方針を追記<br>情報セキュリティ基本方針を情報セキュリティ方針に修正<br>14.1.1 情報セキュリティ基本方針を情報セキュリティ方針に修正 |
| 7.0 版 | 2024.03.01 | 組織変更に伴う部署名の修正<br>5.1.1 情報セキュリティのための方針群 を改訂 |

# 目次

# 1. はじめに

## 1.1. ホワイトペーパーの目的

「UTILIX クラウドサービス ホワイトペーパー」（以降本書と記述）は、ISMS クラウドセキュリティ認証である「JIP-ISMS517-1.0 (ISO/IEC27017:2015)」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。

ISO/IEC 27017 は、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 ISO/IEC 27001 の取組みを ISO/IEC 27017 で強化した管理策のガイドライン規格になります。本書は、このガイドラインの“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）に沿って管理策を記載しています。

## 1.2. 本書の適用範囲

本書の適用範囲は、弊社の UTILIX クラウドサービスとなります。

上記サービスで提供する機能の詳細に関しては、ご利用いただくクラウドサービスのポータルサイト等を参照下さい。

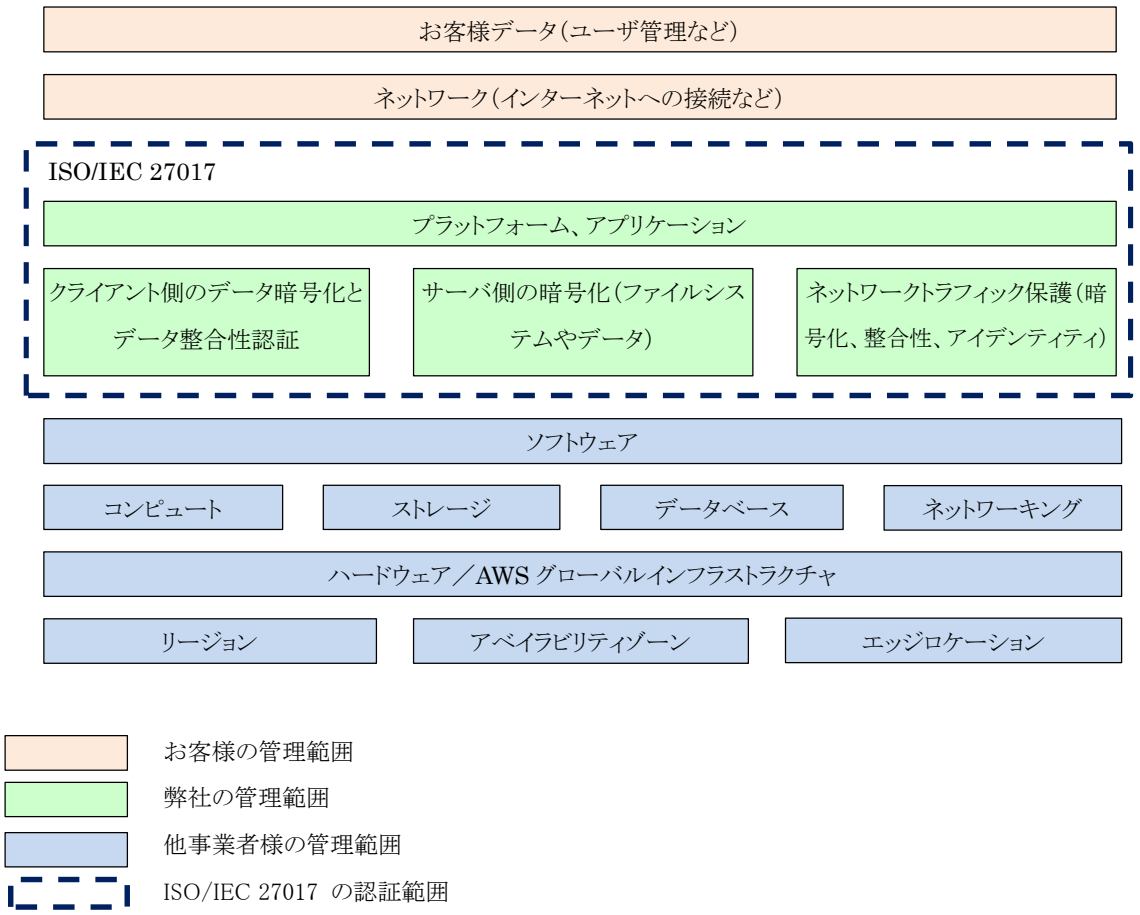
# 2. UTILIX クラウドサービスについて

## 2.1. UTILIX クラウドサービスとは

アズビルが提供する UTILIX クラウドサービスは、アズビルが契約するクラウドサービスプロバイダ(CSP)のクラウドサービス上に、お客様のデータを蓄積し、種々の管理を行う機能を提供します。

## 2.2. 責任分界点について

UTILIX クラウドサービスの責任分界点は、以下になります。



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

## 3.1. UTILIX クラウドサービスの管理策(3.2 節)に関する見方の説明

3.2 節で、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。「5.1.1 情報セキュリティのための方針群」などの番号・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)の小項目番号・要求事項原文を示し、後に続く内容は、UTILIX クラウドサービスの要求事項に対する解釈及び管理策になります。

## 3.2. UTILIX クラウドサービスの管理策

### 5.1.1 情報セキュリティのための方針群

クラウドサービスプロバイダ(CSP)は、クラウドサービスの提供及び利用に取り組むため、情報セキュリティ方針を拡充することが求められています。UTILIX クラウドサービスでは、弊社の情報セキュリティ基本方針、及びグループクラウドサービス部の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。情報セキュリティ基本方針は、弊社ウェブサイトに公開しています。

### 6.1.1 情報セキュリティの役割及び責任

クラウドサービス利用契約書、クラウドサービス利用契約約款及びクラウドサービス仕様書などにて契約やサービスの内容を定義し、サービスを提供しています。

### 6.1.3 関係当局との連絡

弊社のグループクラウドサービス部所在地は、神奈川県藤沢市川名 1-12-2 となります。UTILIX クラウドサービスで保存いただくデータの所在は、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及び責任の共有及び分担

“2.2 責任分界点について”の記述に基づき、弊社が利用しているクラウドサービスプロバイダ(CSP)、クラウドサービス提供者としての弊社、及び弊社のクラウドサービスを利用するお客様の間で、情報セキュリティの役割と責任を分担します。

### 7.2.2 情報セキュリティの意識向上、教育及び訓練

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。

### 8.1.1 資産目録

お客様の情報資産(保存データ)と弊社がクラウドサービスを提供するための情報資産は、明確に分離しています。お客様が UTILIX クラウドサービス上に作成・保存する情報資産は、お客様の管理範囲となります。

### CLD.8.1.5 クラウドサービス利用者の資産の除去

お客様がサービス契約を解約された場合、お客様がクラウドサービス上に作成・保存した情報資産(保存データ)は、サービス解約後原則 1 ケ月以内にデータ及び保管媒体を廃棄します。お客様が情報資産のバックアップなどを必要とされる場合は、お客様からの申し入れに基づき、弊社から提供します。

### 8.2.2 情報のラベル付け

お客様情報資産の分類は、情報を閲覧する際のユーザの権限設定により行うことができます。

### 9.2.1 利用者登録及び登録削除

お客様に提供する管理ツール等を使い、お客様の管理者は、UTILIX クラウドサービスを利用するユーザの登録、登録削除ができます。

### 9.2.2 利用者アクセスの提供（provisioning）

お客様に提供する管理ツール等を使い、お客様の管理者はUTILIXクラウドサービスを利用するユーザに対するアクセス権を管理することができます。

### 9.2.3 特権的アクセス権の管理

特権的アクセス権の管理は、ログイン ID とパスワードによる認証に加えて IP アドレス制限などの多要素認証技術で行うことができます。

### 9.2.4 利用者の秘密認証情報の管理

お客様に提供する管理ツール等を使い、お客様の管理者は、UTILIX クラウドサービスを利用するユーザの秘密認証情報の初期設定や変更ができます。

### 9.4.1 情報へのアクセス制限

お客様の管理者は、管理者ツール等を使ってお客様ユーザのアクセス権の設定ができます。

### 9.4.4 特権的なユーティリティプログラムの使用

お客様は特権的なユーティリティプログラムを利用することができません。

### CLD.9.5.1 仮想コンピューティング環境における分離

マルチテナント環境で動作しますが、ユーザ ID によるアクセス資源の分離を実施し、別テナントへの不正アクセスを抑止しています。

### CLD.9.5.2 仮想マシンの要塞化

仮想マシンを設定する際には，適切な側面からの要塞化（例えば，必要なポート，プロトコル及びサービスだけを有効とする。）及び利用する各仮想マシンへの適切な技術手段（例えば，マルウェア対策，ログ取得）の実施を行っています。

### 10.1.1 暗号による管理策の利用方針

業界標準の AES-256 暗号化アルゴリズムを使用して、Amazon RDS DB インスタンスをホストしているデータをサーバで暗号化します。データが暗号化されると、Amazon RDS はパフォーマンスの影響を最小限に抑えながら、データへのアクセスと復号の認証を透過的に処理します。また、お客様のパスワードは暗号化して保持しています。お客様と提供する UTILIX クラウドサービス間の通信は、TLS 通信による暗号化を行っています。

### 11.2.7 装置のセキュリティを保った処分又は再利用

UTILIX サービスは、弊社が契約するクラウドサービスプロバイダが構築する仮想環境上で提供しており、弊社が直接に処分または再利用を行う資源（装置、データストレージ、メモリ、ファイル）は、保有しておりません。弊社が契約するクラウドサービスプロバイダが、契約に基づき資源の処分または再利用を適切に実施していることを確認しています。

### 12.1.2 変更管理

お客様に通知する必要のある弊社が提供する UTILIX クラウドサービスの仕様変更や仕様追加などについて、お客様向けポータルサイト等で連絡します。その際に実施するメンテナンスについても、同様に連絡します。

### 12.1.3 容量・能力の管理

弊社が契約しているクラウドサービスプロバイダ提供のクラウド環境（弊社のクラウドサービスを提供する基盤となる）上の資源について、容量・能力（ディスク使用率、メモリ使用率、CPU 使用率）を監視し、逼迫している際は資源を拡張し、サービスの提供に影響を与えません。

### CLD.12.1.5 実務管理者の運用セキュリティ

お客様の管理者向けに提供する管理ツール等の取扱説明書と共に、QA サポートも提供し、運用セキュリティを確保いただきます。

### 12.3.1 情報のバックアップ

クラウドサービス上に収集しているお客様の計測データに関するお客様ご自身でのバックアップ機能は、提供しておりません。システム及びお客様情報資産のバックアップは日々の運用プロセスとして実施しております。バックアップは7世代（7日）分のデータを保持し、万が一の障害によりクラウド上のデータが失われた場合は、バックアップデータから復旧することができます。

### 12.4.1 イベントログ取得

クラウド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。お客様が必要とされる場合は、弊社問い合わせ窓口までご相談ください。

### 12.4.4 クロックの同期

システム内はクラウドサービスプロバイダ提供の手法（Amazon Time Sync Service で時間を維持する）で時刻同期されています。

お客様のクライアントマシンの時刻同期が必要な場合は、ローカルネットワークで独自に標準時刻サーバと同期するなどの方法があります。

### CLD.12.4.5 クラウドサービスの監視

弊社は、お客様が利用される UTILIX クラウドサービスが正常に提供され、不正に利用されていないことを、常時監視しています。お客様がサービス運用状況の詳細を確認されたい場合は、弊社問い合わせ窓口までご相談ください。

### 12.6.1 技術的ぜい弱性の管理

弊社は、技術的ぜい弱性の情報を、常時収集しています。お客様の対応が必要となるぜい弱性情報を入手した際は、お客様向けポータルサイト等で必要な対応事項を連絡します。クラウドサービス側の対応が必要となった場合は、弊社が定期または緊急メンテナンスを実施し、セキュリティを確保します。

### 13.1.3 ネットワークの分離

弊社は、ネットワーク間の領域の分離を、適切に行っています。システムを提供するネットワークとデータを保管するネットワークは仮想化技術により分離されています。

### 14.1.1 情報セキュリティ要求事項の分析及び仕様化

弊社は、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機能の仕様として、本書は以下の項目を記述しています

・アクセス制限機能（「9.2.1 利用者登録及び登録削除」）

お客様管理者によるお客様の利用者登録などの機能

・アクセス制限機能（「9.2.2 利用者アクセスの提供(provisioning)」）

お客様管理者によるお客様の利用者に対する設定確認などの機能

・アクセス制限機能（「9.4.1 情報へのアクセス制限」）

お客様管理者によるお客様の利用者のアクセス権設定などの機能

・暗号化機能（「10.1.1 暗号による管理策の利用方針」）

万一の情報漏洩などを想定したリスク評価のための情報

・バックアップ機能（「12.3.1 情報のバックアップ」）

万一のデータ消失などを想定したリカバリのための情報

・ログ取得機能（「12.4.1 イベントログ取得」）

情報セキュリティ事象に際して原因特定などに必要なログが得られることの情報

### 14.2.1 セキュリティに配慮した開発のための方針

弊社は、セキュリティに配慮した開発方針として、開発時点からのセキュリティに関するリスクアセスメントや、ぜい弱性への対策を含む設計指針を策定してクラウドサービスの設計と制作を行い、社内部門であるサイバーセキュリティ室の審査を経て、クラウドサービスを提供しています。

### 15.1.2 供給者との合意におけるセキュリティの取扱い

弊社は、お客様向けに提供するクラウドサービスの情報セキュリティ対策について、本ホワイトペーパーに記述しています。

### 15.1.3 ICT サプライチェーン

弊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、弊社が提供するクラウドサービス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。

### 16.1.1 責任及び手順

弊社が利用するクラウドサービスプロバイダとの責任分界点は、本書「2.2 責任分界点について」で明確にしています。情報セキュリティインシデントは、弊社の情報セキュリティインシデント管理手順に則り、以下のよう適切に管理しています。

・弊社がお客様に報告する情報セキュリティインシデントの範囲

お客様のシステムになんらかの影響を及ぼす事象を範囲とします。

・情報セキュリティインシデントの検出およびそれに伴う対応の開示レベル

弊社に起因する情報セキュリティインシデントでお客様に影響を及ぼすものは、内容に関わらず、すべて同等のレベルで対処します。

・情報セキュリティインシデントの通知を行う目標時間

弊社に起因する情報セキュリティインシデントでお客様に影響を及ぼすものは、1営業日以内にお客様へ通知します。

・情報セキュリティインシデントの通知手順

弊社に起因する情報セキュリティインシデントでお客様に影響を及ぼすものは、お客様向けポータルサイト等で通知します。（状況に応じて電話などの手段を使用する場合もございます）

・情報セキュリティインシデントに関係する事項の取扱いのための窓口の情報

情報セキュリティインシデントに関する窓口は、本サービスの障害・お問合せを受け付ける窓口と同様です。

・特定の情報セキュリティインシデントが発生した場合に適用可能なあらゆる対処

弊社に起因する情報セキュリティインシデントでお客様に影響を及ぼすものは、あらゆる手段を用いて、解決するための対処を行います。

### 16.1.2 情報セキュリティ事象の報告

弊社、または弊社の利用するクラウドサービスプロバイダに起因する情報セキュリティ事象については、お客様向けポータルサイト等で報告します。

### 16.1.7 証拠の収集

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、クラウドコンピューティング環境内で生成される，ディジタル証拠となり得る情報及びその他の情報について、お客様の同意を得ずにこれらの情報を提供する場合があります。

### 18.1.1 適用法令及び契約上の要求事項の特定

本クラウドサービスに関して、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

知的財産権に関するお客様の問い合わせは、本クラウドサービスの問い合わせ窓口までご連絡ください。

### 18.1.3 記録の保護

本クラウドサービスは、クラウドサービスの維持管理に必要となる適切なお客様のアクセス履歴、及びお客様の閲覧履歴を収集、保持しています。お客様が必要とされる場合は、弊社問い合わせ窓口までご連絡ください。

### 18.1.5 暗号化機能に対する規制

暗号の利用は、“10.1.1 暗号による管理策の利用方針” に記述しています。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

弊社は、内部監査、マネジメントレビュー、ISMS リスクアセスメントと管理計画、ISO/IEC 27001 及び ISO/IEC 27017 の ISMS 認証取得を通じて、情報セキュリティの維持、向上を行っています。