Big-Link クラウド

ISO/IEC27017 ホワイトペーパー

2024 年 2 月 26 日（第 3 版）

株式会社東計電算

もくじ

1. はじめに

1.1 本書の目的

本書は、東計電算クラウドプラットフォームサービス（以下、Big-Link クラウド)のご利用者様に、Big-Link クラウドのセキュリティ対策情報を開示・提供することを目的としています。

本書の作成にあたっては、ISO/IEC27017「4.3 クラウドサービスカスタマとクラウドサービスプロバイダとの関係」（クラウドサービスプロバイダは，クラウドサービスカスタマがその情報セキュリティ要求事項を満たすために必要な情報及び技術支援を提供することが望ましい）への対応を意図しました。

なお『Big-Link クラウド』の詳細については、弊社営業担当者までご相談いただくか、弊社サイト（https://www.big-link.biz/）をご覧ください。

1.2 本書で使用する用語について

用語	解説
クラウドサービスプロバイダ	クラウドサービスの提供者。弊社は、『Big-Link クラウド』のクラウドサービスプロバイダに相当します。
クラウドサービスカスタマ	クラウドサービスの利用者。本書では、『Big-Link クラウド』のクラウドサービスカスタマを「ご利用者様」と表記します。

1.3 本書の適用範囲について

弊社が提供する以下のクラウドサービスが、本書の適用範囲となります。

・Big-Link クラウド

　・Big-Link クラウド IaaS

　・ZEP-C1

1.4 ISMS クラウドセキュリティ認証とは

クラウドサービスセキュリティに関する管理策が導入・運用されていることを、第三者機関が審査・証明する認証です。

『Big-Link クラウド』は、以下の規格を適用規格として、管理策を策定しております。

・JIS Q 27017:2016(ISO/IEC 27017:2015)

・ISO/IEC 27017:2015 に基づく ISMS クラウドセキュリティ認証に関する要求事項（JIP-ISMS517-1.0）

2 Big-Link クラウドについて

2.1 Big-Link クラウドについて

Big-Link クラウドは、パブリッククラウドに分類される IaaS（Infrastructure as a Service）です。
以下のサービスから構成されます。

2.1.1 Big-Link クラウド IaaS

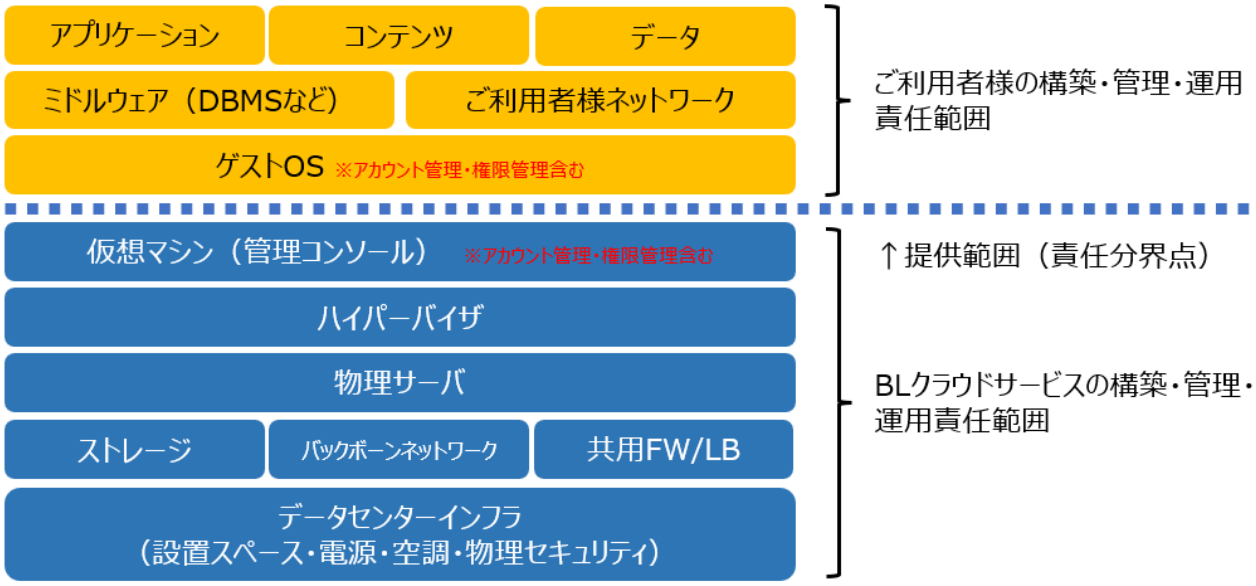
ご利用者様専用のゲスト OS を、弊社クラウド環境に構築・提供するサービスです。

2.1.2 ZEP-C1

Big-Link クラウド IaaS に加え、通信回線・セキュリティ対策・セキュリティオペレーションセンター（SOC）を提供するサービスです。

2.2 責任分界点について

『Big-Link クラウド』における、弊社とご利用者様の責任分界点は、以下の通りです。



※ゲスト OS のインストール及びライセンスの提供が、弊社の責任範囲です。
※ゲスト OS の設定及びアプリケーションは、ご利用者様の責任範囲となります。

上記の責任分界・責任範囲は、以下の要求事項と対応します。

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

CLD 8.1.5　クラウドサービスカスタマの資産の除去

A 9.2.1　利用者登録及び登録削除

A 9.2.2　利用者アクセスの提供

A 9.4.4　特権的なユーティリティプログラムの使用

CLD 9.5.2　仮想マシンの要塞化

A 10.1.1　暗号による管理策の利用方針

A 11.2.7　装置のセキュリティを保った処分又は再利用

A 12.4.4 クロックの同期

CLD 12.4.5　クラウドサービスの監視

A 12.6.1　技術的脆弱性の管理

A 14.2.1　セキュリティに配慮した開発のための方針

A 18.1.5 暗号化機能に対する規制

3. JIP-ISMS517-1.0・ISO/IEC 27017:2015 への対応

3.1　規格に関する見方の説明

3.1.1 JIP-ISMS517-1.0 に関する見方

JIP-ISMS517-1.0 が求める要求事項に対する管理策を記載します。

項目番号・項目名は、JIP-ISMS517-1.0 が定める“要求事項”箇条 4.1～4.3 の小項番番号・規格原文と対応し、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となります。

3.1.2 ISO/IEC 27017:2015 に関する見方

JIS Q 27017:2016（ISO/IEC 27017:2015）に定める実践の規範に対する管理策を記載します。

項目番号・項目名は、ISO/IEC 27017 が定める”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・規格原文と対応し、後に続く内容は、弊社サービスの実践の規範に対する解釈および管理策となります。

ISO/IEC27017 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。

3.2　JIP-ISMS517-1.0 要求事項への対応

4.1　情報セキュリティマネジメントシステムの適用範囲の決定

『Big-link クラウド』サービスのうち、「2.2 責任分界点について」にて弊社の責任範囲として定める領域（クラウドサービスプロバイダとしての責任範囲）を適用範囲として定義します。

4.2　ISO/IEC 27017 の規格に沿ったクラウド情報セキュリティ対策の実施

当データセンターの適用範囲における業務活動及びリスクとの関連のもとに、JIS Q 27017:2016(ISO/IEC 27017:2015)の規格に沿った、文書化されたセキュリティ対策を確立し、実施・維持及び継続的改善を行います。

4.2.1　情報セキュリティリスクアセスメント

弊社は下記の手順でリスクアセスメントを実施します。

1)適用範囲における情報資産と資産価値の特定
2)情報資産に対する脅威の特定
3)脅威によって利用されるおそれのある脆弱性の特定
4)機密性、完全性及び可用性の喪失による情報資産への影響の特定
5)実施されている管理策と、情報資産に対する脅威及び脆弱性による影響が実際に起こる可能性からリスク値を算定
6)リスクの受容が可能か、対応を必要とするかを決定

4.2.2　情報セキュリティリスク対応

弊社は、下記の手順でリスク対応を実施します。

1)リスクの低減・回避・受容・転嫁いずれかの対応を、「リスクアセスメント基準」に従い選択
2)リスク対応のための管理目的・管理策の選択
3)2)で選択した管理目的・管理策を、JIS Q 27017:2016(ISO/IEC 27017:2015)に示す管理策と比較・検証
4)適用宣言書を作成
5)残留リスクに対する受容、もしくは管理策導入を検討

4.3　内部監査

弊社は、クラウドセキュリティ管理策・プロセス及び手順について、以下の観点から、年 2 回内部監査を実施します。

1)JIP-ISMS517-1.0、JIS Q 27017:2016 の規格及び関連する法令・規制等へ適合していること。
2)クラウドセキュリティ管理策・プロセス及び手順が有効かつ期待通りに実施され、維持されていること。

3.3　ISO/IEC 27017:2015 管理策の実践の規範への対応

5.1.1 情報セキュリティのための方針群

弊社がクラウドサービスを運営するにあたり、情報セキュリティ方針を定めています。

情報セキュリティ方針は、従業員及び関係者への通知と、定期的な見直しを行い、安全性の高いクラウド環境の提供に努めています。

6.1.1 情報セキュリティの役割及び責任

『Big-Link クラウド』のご利用に際しての、役割・責任は以下の通りです。

責任項目	Big-Link クラウド	ZEP-C1
一次障害調査・一次復旧対応	弊社	弊社
セキュリティ監視	ご利用者様	弊社
死活監視・リソース閾値監視	弊社	弊社
サーバ・ネットワーク構成管理	ご利用者様	弊社
外部ファイアウォール IPS・内部ファイアウォール	ご利用者様	弊社
インターネット接続回線	ご利用者様	弊社
ご利用者様のネットワーク	ご利用者様	弊社
コンテンツ・データ	ご利用者様	ご利用者様
アプリケーション	ご利用者様	ご利用者様
ミドルウェア（Web サーバ、DBMS など）	ご利用者様	ご利用者様
ゲスト OS	ご利用者様	ご利用者様
仮想マシン（管理コンソール）	弊社	弊社
ハイパーバイザ	弊社	弊社
物理サーバ	弊社	弊社
ストレージ・バックボーンネットワーク・共用 FW/LB	弊社	弊社
データセンターインフラ	弊社	弊社

6.1.3 関係当局との連絡

『Big-Link クラウド』のデータ保存場所は、東計電算データセンター（日本国内）です。

『ZEP-C1』サービスにおけるセキュリティ事象解析（SOC としての機能）は、「2.2 責任分界点について」にて定める弊社責任範囲と「ゲスト OS」のログ検査を、日本国外で実施する可能性があります。

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分担

『Big-Link クラウド』利用にあたり役割・責任は、「2.2 責任分界点について」にて定める弊社とご利用者様の責任範囲に準じます。

7.2.2 情報セキュリティの意識向上、教育及び訓練

弊社としては情報セキュリティ方針を定め、日々サービスを運営しています。また本サービスの従事者に対し、職務に関する方針及び手順については定期的な教育・訓練を実施しております。

8.1.1 資産目録

ご利用者様の情報資産（ご利用者様にて保存されるデータ）と、弊社がサービスを運営するための情報は、明確に分離しております。

なお、ご利用者様の情報資産につきましては、ご利用者様の管理範囲となります。

CLD.8.1.5 クラウドサービスカスタマの資産の除去

仮想マシンの削除は、ご利用者様からの解約申込後に、弊社が実施いたします。

「2.2 責任分界点について」にて示す、ご利用者様の管理・責任範囲のすべてと、弊社管理責任範囲の『仮想マシン（管理コンソール)』が削除対象となります。

8.2.2 情報のラベル付け

『Big-Link クラウド』では、仮想マシン上に保存されたデータに対してラベル付けを行う機能は提供しておりません。お問い合わせをいただいたご利用者様には、ラベル付けの為の情報提供が可能です。

9.2.1 利用者登録及び登録削除

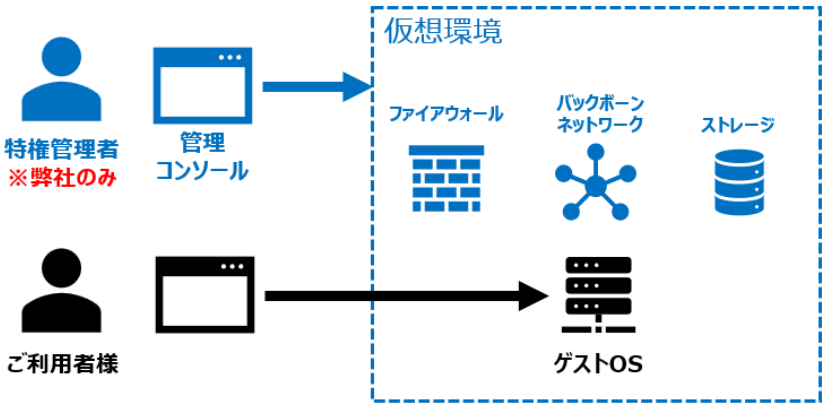
『Big-Link クラウド』から提供される仮想マシンの登録・削除は、弊社にて実施いたします。ご利用者様から登録・削除を行う機能は提供しておりません。

9.2.2 利用者アクセスの提供

『Big-Link クラウド』のユーザ権限を管理する機能は提供しておりません。アクセス提供に関しては、前項「2.2 責任分界点について」と次項「9.2.3 特権的アクセス権の管理」にて参照ください。

9.2.3 特権的アクセス権の管理

『Big-Link クラウド』管理コンソールへのアクセス権は、弊社の特権管理者のみが保有し、ご利用者様には特権的アクセス権を提供いたしません。



9.2.4 利用者の秘密認証情報の管理

ご利用者様の秘密認証情報は、「2.2 責任分界点について」にて示す、ご利用者様の管理・責任範囲となります。ご利用者様にて管理をお願いいたします。

9.4.1 情報へのアクセス制限

『Big-Link クラウド』の仮想マシン（管理コンソール）へのアクセスは、弊社の閉域ネットワークからのみ許可しています。インターネット(VPN 等含む）では提供しておりません。

9.4.4 特権的なユーティリティプログラムの使用

『Big-Link クラウド』においては、ご利用者様に、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行っておりません。「2.2 責任分界点について」にて示す、仮想マシン(管理コンソール)、ハイパーバイザは、弊社の特権管理者が管理を行います。

CLD.9.5.1 仮想コンピューティング環境における分離

『Big-Link クラウド』で提供される仮想マシン（管理コンソール)、ゲスト OS は、仮想化技術を使用し、ご利用者様ごとに、論理的な分離を実施しております。

CLD.9.5.2 仮想マシンの要塞化

『Big-Link クラウド』サービスの外部から、ゲスト OS へ通信を行う場合は、ゲスト OS 上の FW にて、通信を許可する設定が必要です。このゲスト OS 上の FW 設定は、ご利用者様にて実施していただきます。また、弊社の責任範囲となる共用 FW での設定変更が必要となる場合、弊社にて設定を行います。ホストマシン上のゲスト OS のネットワークは、ご利用者様単位で VLAN を作成し、ネットワークが分割されている為、ご利用者様間の環境を横断してのアクセスは不可能です。ゲストＯＳの要塞化は、ご利用者様にてサービスの導入やログ取得の実施が可能です。

10.1.1 暗号による管理策の利用方針

『Big-Link クラウド』で提供する仮想マシンには、ご利用者様にて実施可能な暗号化機能を提供しておりません。『Big-Link クラウド』ご利用者様の定めるポリシーに基づき運用する事が可能となっております。

11.2.7 装置のセキュリティを保った処分又は再利用

『Big-Link クラウド』内の資源（ストレージ、メモリ）の再利用は、ご利用者様のデータが削除された領域に対してのみ行われます。

故障・利用終了に伴って装置の廃棄を行う場合、装置内の記憶媒体に対して、弊社取扱基準にて定める期日までに、破砕処分を実施しています。また、『Big-Link クラウド』の記憶装置は、RAID 化技術により、仮想ストレージを構成しているため、ディスク単体では、ストレージ内に保存された情報の取得は不可能です。

12.1.2 変更管理

『Big-Link クラウド』のサービス停止を伴うメンテナンスは、ご利用者様に事前に通知を行った上で実施いたします。

緊急のメンテナンスについては、事前通知を行わずに実施される可能性があります。

12.1.3 容量・能力の管理

ご利用者様の要望に応じて、『ゲスト OS』の CPU、メモリ、ネットワーク利用量、トラフィック総量等の監視を行います。物理サーバー・ストレージ・バックボーンネットワーク等の、サービス提供基盤についても、リソース使用状況・稼働状況を監視します。

CLD.12.1.5 実務管理者の運用のセキュリティ

『Big-Link クラウド』サービスでは、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。もし情報セキュリティ事故が発生した場合には、速やかにご担当者様宛にご連絡いたします。

12.3.1 情報のバックアップ

『Big-Link クラウド』に異常が発生した際、復旧が行えるよう、基盤環境の設定情報を保持しています。

「2.2 責任分界点について」、「6.1.1 情報セキュリティの役割及び責任」にて示す弊社責任範囲が、弊社のバックアップ対象です。

12.4.1 イベントログ取得

「2.2 責任分界点について」にて示す、弊社責任範囲のイベントログを取得しています。

仮想マシンごとのイベントログをご利用者様のご要望に応じて開示いたします。

12.4.4 クロックの同期

「2.2 責任分界点について」にて示す、弊社責任範囲の機器に対して、弊社が管理する NTP サーバを参照し、クロック同期を行っています。

CLD.12.4.5 クラウドサービスの監視

『Big-Link クラウド』では、ご利用者様から、直接の仮想マシンのＣＰＵ、メモリ、ネットワークの利用量等を参照は出来ませんが、ご利用者様の希望に応じ、ログの提示は可能です。詳細は『Big-Link クラウド利用規約』を参照ください。

12.6.1 技術的ぜい弱性の管理

「2.2 責任分界点について」にて示す、弊社責任範囲内のぜい弱性を、定期的にベンダーサイトより確認しています。

サービス提供機器やソフトウェアのぜい弱性が発見され、影響が発生する場合には、情報収集、対策実施とともに、ご利用者様への対応連絡を行います。

13.1.3 ネットワークの分離

『Big-Link クラウド』では、ご利用者様ごとに論理的にネットワークを分離し、弊社責任範囲のネットワークに関しても、ご利用者様のネットワークと分離しています。

CLD.13.1.4 仮想及び物理ネットワークのセキュリティ管理の整合

『Big-Link クラウド』においては、弊社が定めるネットワーク構築基準に基づき、仮想・物理を問わず、同様のネットワーク管理を実施しています。

14.1.1 情報セキュリティ要求事項の分析及び仕様化

『Big-Link クラウド』では、オプションサービスとして、FW、不正侵入検知（IPS）、アンチウィルス、Web フィルタリング、SOC サービスの提供が可能です。詳細は『Big-Link クラウド利用規約』を参照ください。

14.2.1 セキュリティに配慮した開発のための方針

「2.2 責任分界点について」にて示す、『ゲスト OS』『ミドルウェア』『アプリケーション』『データ』『コンテンツ』に関しては、ご利用者様の管理・責任範囲となります。

15.1.2 供給者との合意におけるセキュリティの取扱い

弊社が利用する供給者については、弊社の外部委託に関する基準に従い、管理を行っています。

15.1.3 ICT サプライチェーン

弊社からの委託先については、弊社の外部委託に関する基準に従い、管理を行っています。

16.1.1 責任及び手順

『Big-Link クラウド』サービスにて確認されたインシデントは、弊社内の運用手順に基づき、契約時に連絡先を取り交わす弊社営業担当者より、通知を行います。

16.1.2 情報セキュリティ事象の報告

『Big-Link クラウド』サービスに関する情報セキュリティ事象の問い合わせは、弊社内でインシデント管理を行っています。

『Big-Link クラウド』サービスで発生した情報セキュリティ事象は、契約時に連絡先を取り交わす弊社営業担当者より、ご利用者様に報告を行います。

ご利用者様から弊社に情報セキュリティ事象をご報告いただく場合は、契約時に取り交わす連絡先、もしくは、弊社サイト（https://www.big-link.biz/）に記載の電話番号・お問い合わせフォームより、ご連絡ください。

16.1.7 証拠の収集

登録が確認のできたご利用者様より、情報開示のご要望をいただいた際は、情報を提供いたします。

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場合、ご利用者様の同意なく、情報を開示する可能性があります。

18.1.1 適用法令及び契約上の要求事項の特定

『Big-Link クラウド』のサービス利用に関する準拠法は、日本法とします。

18.1.2 知的財産権

『Big-Link クラウド』内にて、知的財産権のあるソフトウェアをご利用頂く場合は、契約時に取り交わす連絡先、もしくは、弊社サイト（https://www.big-link.biz/）に記載の電話番号・お問い合わせフォームより、ご連絡ください。

18.1.3 記録の保護

「2.2 責任分界点について」にて示す、弊社責任範囲内の記録の保護を実施いたします。
ご利用者様の責任範囲の記録につきましては、ご利用者様にて保護を行っていただきます。

18.1.5 暗号化機能に対する規制

「2.2 責任分界点について」にて示す、弊社責任範囲のネットワーク内の通信は、SSL 暗号化を実装しております。輸出規制の対象となる暗号化の利用はありません。
ご利用者様の責任範囲内の暗号化機能は、ご利用者様により、実装・管理を行っていただきます。

18.2.1 情報セキュリティの独立したレビュー

以下の各事項を実施しています。

- IS0/IEC 27001 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いることで、情報セキュリティに対する取り組みの証憑としています。
- Big-Link クラウドのご利用を検討される事業者様、およびご利用者様の定めるセキュリティチェックシート等について、回答を行っています。
- 弊社データセンターは、施設見学の受け入れを行っており、建物設備や運用についてご見学いただくことができます。
- 本書により情報の開示を行っています。

4.改訂履歴

版　数	変更改訂日	改訂・変更の理由および内容
01	2022.11.14	初版発行
02	2023.02.24	A 8.2.2、A 9.2.2、CLD9.5.2、A 10.1.1、11.2.7、CLD 12.1.5 、CLD 12.4.5、A 14.1.1 更新
03	2024.02.26	A 6.1.3、更新