FUJITSU Hybrid IT Service FJcloud-O / FJcloud-ベアメタル セキュリティ関連情報

富士通株式会社

2020年10月30日

Version 1.5.9

まえがき（1/2）

○ 本書の目的

本書では、FUJITSU Hybrid IT Service FJcloud-O / FJcloud-ベアメタル（旧称FUJITSU Cloud Service for OSS) (※以降　FJcloud-O / FJcloud-ベアメタルまたは本サービス)の利用をご検討頂いている方に、

本サービスにおけるセキュリティの考え方を理解していただくことを目的としています。

なお、本書ではサービス機能に関しては、FJcloud-O / FJcloud-ベアメタル IaaSについて記載しております。

○ 前提知識

以下の知識があることが望ましい

- OSに関する基本的な知識
- インターネット、イントラネットに関する基本的な知識
- セキュリティに関する基本的な知識
- バックアップ、監視、冗長化などシステム設計/システム運用に関する基本的な知識

まえがき（2/2）

FUJITSU

- 商標登録について
  - 記載されている会社名、製品名等の固有名詞は各社の商号、登録商標または商標です。
  - その他、本資料に記載されている会社名、システム名、製品名等には必ずしも商標表示を付記しておりません。

- 著作権・商標権・その他の知的財産権について
  - 本資料は、著作権・商標権・その他の知的財産権で保護されています。本資料を形式、手段(電子的又は機械的)、目的に関係なく、当社の書面による事前の承諾なく、複製、内容の改変、又は転載することを禁止します。

- 免責事項
  - 本資料は、本資料公開日時点の情報をもとに記載しています。
  - 本資料は、単に情報として提供され、内容は予告なしに変更・廃止されることがあります。
  - 本資料について、当社は、その正確性、商品性、利用目的への適合性を保証しません。
    明示的又は黙示的な保証や条件は、一切無いものとします。
  - 本資料について、当社は、いかなる責任も負いません。
    本資料により、直接又は間接にいかなる契約上の義務も負うものではありません。
  - 本資料に記載された記載内容の使用に起因する 第三者の特許権 および その他の権利の侵害については、当社はその責を負いません。

- 輸出管理規制について
  - 本資料を輸出又は第三者へ提供する場合は、お客様が居住する国および米国輸出管理関連法規等の規制を、ご確認のうえ、必要な手続きをおとりください。

変更履歴

版数	更新日	変更内容
1.0	2017年5月11日	初版作成
1.1	2017年6月20日	雷対策について追記(p.15)、VLANに関する補足追記(p.22)、認証・規格対応状況最新化(p.39)
1.2	2017年7月28日	文章表現修正(p.22、27)、認証・規格対応状況最新化(p.39)
1.3	2017年8月18日	文章表現修正(p.2、17)、認証・規格対応状況最新化(p.39)
1.4	2017年10月3日	文章表現修正(p.16、17)、説明内容最新化(p.33)
1.4.1	2017年11月10日	認証・規格対応状況最新化(p.39)
1.4.2	2017年12月22日	認証・規格対応状況最新化(p.39)
1.5	2018年1月26日	表現修正（p.22）、認証・規格対応状況修正(p.39)
1.5.1	2018年2月16日	認証・規格対応状況最新化(p.39)
1.5.2	2018年3月19日	認証・規格対応状況最新化(p.39)
1.5.3	2018年6月11日	認証・規格対応状況最新化(p.39)
1.5.4	2018年12月21日	認証・規格対応状況最新化(p.39)、サービス名称変更
1.5.5	2019年3月1日	認証・規格対応状況最新化(p.39)
1.5.6	2019年4月11日	認証・規格対応状況を富士通公開サイトへのリンクに変更(p.39)
1.5.7	2020年2月17日	説明最新化・修正（P.17,P.18,P.19,P.25,P.33,P.40）、文章表現修正（P.31,P.34）、4.2章ページタイトル変更（P.34~37）、認証・規格対応状況のリンク先URLを最新化（P.39）
1.5.8	2020年6月11日	サービス名称変更
1.5.9	2020年10月30日	サービス名称変更（FJcloud-ベアメタルを併記）、セキュリティ推進体制の組織名の変更(p.32,p.34,p.36)

目次

第1章　はじめに ····· 5
1.1　情報セキュリティとは ····· 6
1.2　クラウドにおける情報セキュリティの考え方 ····· 7
1.3　IaaSサービスの責任分解点 ····· 9

第2章　クラウド基盤に対するセキュリティ確保の取組み ····· 10
2.1　概要 ····· 11
2.2　データセンターとしての対策 ····· 12
2.3　ネットワークに対する対策 ····· 16
2.4　物理ストレージに対する対策 ····· 18
2.5　物理サーバに対する対策 ····· 20
2.6　仮想化基盤に対する対策 ····· 22

第3章　セキュアにご利用頂くために提供する機能 ····· 24
3.1　概要 ····· 25
3.2　利用環境管理に関するセキュリティ機能 ····· 26
3.3　仮想マシン環境に関するセキュリティ機能 ····· 27
3.4　仮想ストレージに関するセキュリティ機能 ····· 28
3.5　仮想ネットワークに関するセキュリティ機能 ····· 29

第4章　セキュリティ推進体制と取組み ····· 30
4.1　セキュリティ推進体制 ····· 31
4.2　サービス基盤セキュリティ運用 ····· 34

第5章　各リージョンに関する情報 ····· 38
5.1　認証・規格への対応状況 ····· 39
5.2　各リージョンの法制度 ····· 40

付録　用語説明 ····· 41

FUJITSU

第１章　はじめに

1.1 情報セキュリティとは

OECDが1992年に発表した「情報セキュリティのためのガイドライン」(※注1～注3) では、情報セキュリティの目的を以下のように定めています。

「情報システムセキュリティが目的とするのは、可用性、機密性、完全性が不十分であることから生じる危害から、情報システムを信頼している人たちの関心を保護することである」

ここでいう、機密性、完全性、可用性は以下のように定義されています。

- ・機密性（Confidentiality）：データや情報が、正当な時に、正当な手順によって、正当な権限を持つ人・実体・プロセスだけにのみ公開されること
- ・完全性（Integrity）：データや情報が、正確かつ完全である状態が保たれること
- ・可用性（Availability）：データや情報、情報システムが必要なときに、必要な手順に従ってアクセスできること

これらは、英語の頭文字をとってCIAと呼ばれ、「情報セキュリティの三要素」といわれています。
システムを構成する各要素、および、システムの運用において、「情報セキュリティの三要素」を意識し、対策を積み重ねることが、情報システム全体のセキュリティを高めるためには重要になります。

(注1) OECD Guidelines for the Security of Information Systems, 1992
http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm
(注2) OECD 情報セキュリティガイドライン見直しに関する調査：注1資料の日本語サマリ
https://www.ipa.go.jp/security/fy14/reports/oecd/oecd-security.pdf
(注3) Digital Security Risk Management,2015 ：OECDのセキュリティガイドラインの最新(2015年)版
http://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm

1.2 クラウドにおける情報セキュリティの考え方 (1/2)

一般的にクラウドを利用してシステムを運用する場合、クラウド固有の情報セキュリティの考え方を理解しておく必要があります。

まず、クラウド(IaaS)では、システム管理者が管理可能なシステム構成要素は、
オンプレミス上(お客様自身の環境など)でシステムを運用する場合と大きく異なります。

システムの構成要素（比較観点）	オンプレミス上のシステム	クラウド上のシステム
物理的な機器の設置施設	情報システム部門などのシステム管理者が管理	クラウドサービス事業者が管理 （利用者は関与できない）
物理的な機器の維持管理 (物理サーバ、ネットワーク機器 など)	情報システム部門などのシステム管理者が管理	クラウドサービス事業者が管理 （利用者は関与できない）
仮想化基盤の管理	情報システム部門などのシステム管理者が管理	クラウドサービス事業者が管理 （利用者は関与できない）
OSや、ミドルウェア、業務アプリケーションなどの仮想サーバ環境の維持管理	情報システム部門などのシステム管理者が管理	クラウドサービス利用者が管理 (クラウドの提供機能やOS標準機能、 サードパーティ製のソフトウェアを利用して管理)
ファイアウォールなどのネットワーク利用環境の設定	情報システム部門などのシステム管理者が管理	クラウドサービス利用者が管理 (クラウドの提供機能やOS標準機能、 サードパーティ製のソフトウェアを利用して管理)

1.2 クラウドにおける情報セキュリティの考え方 (2/2)

これを、情報システムのセキュリティ管理の観点でメリット・デメリットをまとめると以下のようになります。

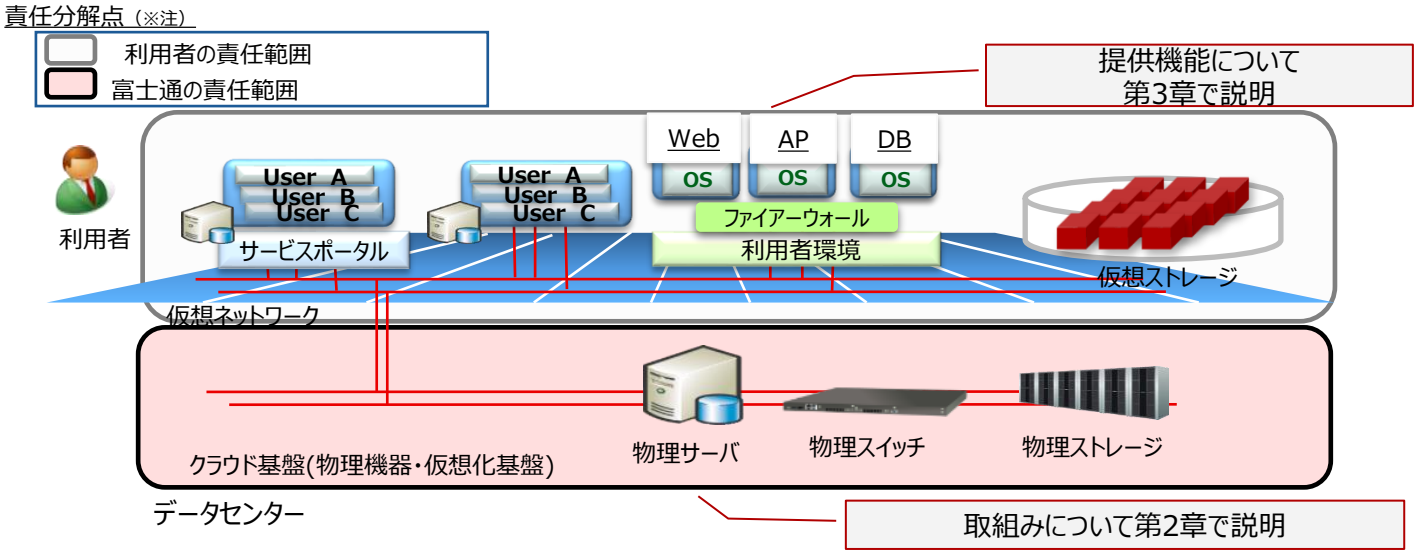
システムの所在	メリット	デメリット
オンプレミス上のシステム	情報システムを構成するすべてのシステム構成要素をシステム管理者自身で管理可能なため、システムに必要となるセキュリティレベルを自ら定めて、適切に対処できる。	情報システムを構成するすべてのシステム構成要素の運用を自分たちで行う必要がある。
クラウド上のシステム	システム管理者(クラウドサービス利用者)は、物理機器を管理するための設備や、物理機器・仮想化基盤に関する運用（ハード故障への対応やファームウェア・セキュリティパッチの適用など）から解放される。 なお、仮想サーバ環境の管理や、ネットワーク利用環境の設定は、従来どおりシステム管理者が運用管理する必要がある。	システム管理者(クラウドサービス利用者)は、クラウドサービス提供者が管理する設備や、物理機器・仮想化基盤について、きちんとセキュリティを保った運用管理を行っているものと信頼して、サービスを利用することしかできない。

つまり、一般的に、クラウドサービスを利用する場合、クラウドサービスの提供者とクラウドサービスの利用者がお互いの責任分解点を理解した上で、相互に協力してシステム全体のセキュリティを確保する必要があります。

クラウドサービスを利用する場合には、このような考え方を理解しておくことは非常に重要になります。

1.3 サービスの責任分解点

- サービスを利用する場合の責任分解点は以下のとおりです。
  - 物理機器を配置するファシリティ(データセンター)、物理機器、仮想化基盤については、富士通の責任範囲となります。
    これらに対するセキュリティ確保の取組みについては、本書の2章で記載します。
  - サービス利用者の管理、および、サービスにより提供されたシステムの各構成要素（OS、ミドルウェア、仮想ストレージ、ファイアウォールなど）の設定・運用管理や業務アプリケーションの管理、監視については、サービス利用者の責任範囲となります。
    これらをセキュアにご利用頂くために提供している機能については、本書の3章で記載します。



※ 注）正式な情報は、本サービス利用規約をご参照下さい。

第２章　クラウド基盤に対するセキュリティ確保の取組み

2.1 概要

2章では、クラウド基盤をセキュアな状態でお客様に提供するために、データセンターやクラウド基盤の構成要素（ネットワーク、物理ストレージ、物理サーバ）で、どのような技術的あるいは運用上の対策を施しているのかを、以下の「情報セキュリティの三要素」の観点に添う形で記述します。

- 機密性 (第三者による不正アクセス対策)
- 完全性 (データの改ざん防止、証跡の管理)
- 可用性 (単一障害点の回避)

※2章の記述に関する注意事項

- 2.2節で記載するデータセンターについては、東日本リージョン１を対象として記載します。

  （各リージョンとも、ほぼ同様の施策を実施しています。）

- 2.3節以降で記載する物理機器（ネットワーク、物理ストレージ、物理サーバ）、仮想化基盤の記述に関しては、スタンダードサービスで利用するコンピュート、ストレージ、ネットワークを対象としています。

  「専有物理サーバサービス」「ベアメタルサービス」に関しては、本書では記述していません。

2.2 データセンターとしての対策（1/4）

東日本リージョンの例です

○ 機密性

データセンターでは、外部の第三者が物理的にデータセンターに侵入できないように、以下のような施策を実施しています。

外周赤外線センサー監視

・外周に赤外線センサーを設置

異常発生時は自動的にカメラで記録され、
警備員がすぐに駆け付けられる運用体制

高精度監視

・高機能カメラにより、昼夜問わず高精度な監視を実施
・モーション検知により異常状態を検知

24時間有人監視

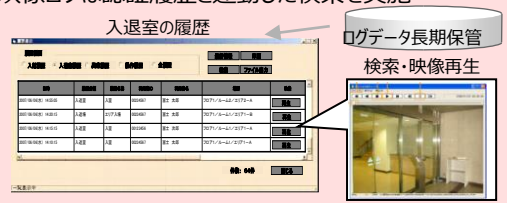
・24時間有人による監視を実施

警備員が24時間待機

※警察署と共同で
年2回防犯訓練実施

ログ管理・トレース

・監視映像、入退室ログを長期間保管
・映像ログは認証履歴と連動した検索を実施



2.2 データセンターとしての対策 (2/4)

FUJITSU

○ 機密性

東日本リージョンの例です

また、データセンターに出入りできる作業従事者であっても、有資格者以外が環境にアクセスできないよう、以下の施策を実施しています。

セキュリティーエリアの設定

・センター内に複数のセキュリティエリアを設定
・入館者は入室資格に応じた区域のみに立入り可能

ラックセキュリティ

・手のひら静脈認証でラック施錠／解錠管理
・センター提供ラックはラックハンドルを電気錠化

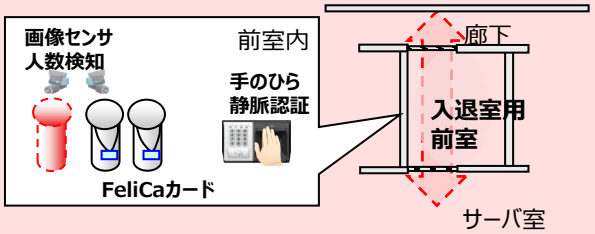
入退室管理

・手のひら静脈認証装置による生体認証を実施

手のひら静脈認証の認証精度
=
他人受入率
0.00008%以下
（125万人に一人）

サーバ室入館時の共連れ防止

・ FeliCaカード、動線カメラ、生体認証を連動させ、共連れを防止



2.2 データセンターとしての対策 (3/4)

FUJITSU

- 完全性
  - クラウド基盤に対する証跡管理

東日本リージョンの例です

正当なアクセス権限を持った運用担当者が、故意、または、過失によって、クラウド基盤に対する改ざんや情報の漏洩が行われないよう、証跡管理を実施しています。

障害、またはセキュリティインシデントが発生した場合には、これら証跡を利用した原因追求および対策が行われます。
なお、これらのログや証跡に関する情報はクラウド基盤に関する内部の情報となりますので、サービス利用者への提供は行っていません。

証跡分類	定義	実施内容
1)マネジメント状況把握型	情報セキュリティマネジメントシステムやマネジメントプロセスが正しく機能していることを確認するための証跡。	内部作業や作業の当社承認履歴の保管。
2)コントロール状況把握型	個々の情報セキュリティ対策が正しく機能していることを確認するための証跡。	お客様共通機能／物理インフラ環境のセキュリティ対策作業ログの保管
3)セキュリティ不正検知型	不正な行為によって個々の情報セキュリティ対策が脅威に面していることを知らせるための証跡。	システム基盤に対するIDS(侵入検知システム)による不正アクセス検知ログの保管
4)セキュリティ追跡性確保型	不正な行為があったときに、その行為の内容や影響範囲を事後的に確認するための証跡。	1）、2）、3）のログを長期保管し、遡及的な調査が実施可能な体制を整えております。

2.2 データセンターとしての対策 (4/4)

FUJITSU

○ 可用性

東日本リージョンの例です

利用者が必要な時にリソースを利用できるよう、以下の取組みを行っています。

- ○ 日本国内については、ティア3(※注１)相当以上のデータセンターで運用しており、地震対策、水害対策(浸水、漏水、渇水、結露)、停電対策、火災対策などの各種対策を施しています。
- ○ 電源系統、空調設備の異なる施設をアベイラビリティゾーンとして複数提供し、電源系統、空調障害によるアベイラビリティゾーンのダウンに対しても業務継続可能な仕組みを提供しています。
- ○ 広域障害発生時でも業務継続可能な仕組みを提供するため、複数のリージョン（データセンター）でサービスを提供しています。

地震対策	水害（浸水、漏水、渇水、結露）対策
・免震構造（建屋、付帯設備） ・支持基盤は積層砂礫質土層の強固な地層	・一階床高さ地上３．７ｍ設計 ・漏水センサー設置 ・空調用補給水１，４００ｔ備蓄 ・専用一時保管庫設置（温度調整による結露防止）
停電対策	**火災対策**
・変電所分離、二系統受電 ・UPS冗長化 ・自家発電設備設置	・Ｎ２（窒素）消火設備設置 ・超高感度煙センサー設置 ・消防署至近（最短７分、年２回共同訓練実施） ・雷対策（保護レベルⅠ、ＪＩＳ Ａ ４２０１）

(※注1)ここでいう「ティア」は、JDCC（Japan Data Center Council：日本データセンター協会）が定めたデータセンターファシリティスタンダードに基づく。
詳細は下記の資料をご参照ください。
日本データセンター協会：データセンターファシリティスタンダードの概要
http://www.jdcc.or.jp/pdf/facility.pdf

2.3 ネットワークに対する対策(1/2)

FUJITSU

- 機密性

  クラウド基盤に対する電子的な外部侵入者（クラッカーなど）への対策としては、以下のような取組みを行っています。

  - IDS(侵入検知システム)を設置することで、クラウド基盤に対する外部からの不正アクセスを24時間無停止で監視しています。
    セキュリティインシデントが疑われる場合には、関係者に自動的に通知が行われ、対策を施すように運用ルールが定められています。
    なお、IDSによる不正アクセス監視は、個々の利用者環境に対しては、対象外となっています。

  - サービス提供時には、富士通内のセキュリティ専門部署による監査を受け、既知の脆弱性がないことをサービス提供に関与していない第三者の視点で確認しています。

2.3 ネットワークに対する対策(2/2)

FUJITSU

- 完全性
  - ネットワーク通信の暗号化

クラウド基盤の運用上発生するネットワーク内の通信は、運用上必要な一部の通信を除いて、すべての通信を暗号化しています。
現在暗号化していない通信も、今後暗号化していく方針です。

※注意※
クラウド基盤の運用上発生する通信は暗号化していますが、サービス利用者が行う通信を自動的に暗号化する機能を提供するものではありません。

- 可用性
  - ネットワーク機器の冗長構成

クラウド基盤内の物理的なネットワーク機器は冗長構成をとっています。物理ネットワークを用いて構成される仮想ネットワークも冗長構成となっています。（※注：東日本1/2、西日本1/2ﾘｰｼﾞｮﾝの仮想ネットワークは一部異なりますが、常時監視を行い、障害発生時には正常な基盤に切り替えられます）

また、インターネットへ接続するネットワーク機器も冗長構成をとっています。ただし、インターネットへ接続する機器に障害が発生した場合には、ルーティングの切り替え処理が発生するため、通信断が発生することがあります。

2.4 物理ストレージに対する対策(1/2)

FUJITSU

○ 機密性

○ 物理ストレージへの物理的なアクセスの制限

物理ストレージ上にあるディスクドライブの盗難防止のため、物理ストレージを搭載したラックは電気錠化しています。
本サービス運用上の有資格者が、生体認証を経てラックの電気錠を開錠しないと、物理ストレージにアクセスできないように運用しています。

○ 物理ディスクドライブの暗号化による情報漏えい対策

ストレージに格納されているデータは、以下のいずれかの方式により暗号化しております。

・自己暗号化ドライブ(SED)を用いて、データをディスクドライブに書き込む際に暗号化を行います。暗号化鍵はディスクドライブからは取り出せません。

・ストレージ装置のファームウェアが、データをディスクドライブに書き込む際に暗号化します。暗号化鍵はファームウェアからは取り出せません。

どちらの方式においても、暗号化の認証に使用する認証鍵は鍵管理サーバまたはストレージ装置が管理しています。
そのため、ディスクドライブを物理ストレージから物理的に取り出した状態では、データを復号することはできません。
ディスクドライブの交換・廃棄を行う場合には、ディスクドライブの破壊は行っていませんがデータの復元が不可能な状態で廃棄しています。

※注意※

暗号化はディスクドライブ全体に対して行われます。ディスクドライブ上の個々のデータに対する暗号化は行いません。
サービス利用者が仮想ストレージ上のデータを扱う際には、常に透過状態（ディスクドライブ全体に対する暗号化を意識しない）で閲覧可能です。
仮想ストレージ上の個々のデータを暗号化する必要がある場合にはサービス利用者自身にて、データ暗号化の方式を検討する必要があります。

2.4 物理ストレージに対する対策(2/2)

FUJITSU

- 完全性
  - 物理ストレージ操作の証跡管理

    物理ストレージに対する不正な運用・管理操作(ディスクドライブの取外しなど)を検知した場合、クラウド基盤の運用者に通報する仕組みを備えています。ストレージ操作に関する証跡ログは一定期間保存されており、不正操作に対する原因を追究することができる仕組みを整えています。

- 可用性
  - ディスクドライブの冗長構成

    ストレージ装置および物理ディスクドライブは、冗長構成によりお客様データが保持されるよう対策しております。

2.5 物理サーバに対する対策(1/2)

- 機密性
  - 物理サーバへの物理的なアクセスの制限

    物理サーバへの物理的なアクセスを有資格者のみに制限するために、物理サーバを搭載したラックは電気錠化しています。
    本サービス運用上の有資格者が、生体認証を経てラックの電気錠を開錠しないと、物理サーバには物理的にアクセスできないように運用しています。

  - 物理サーバに対するリモートアクセスの制限

    物理サーバに対するネットワーク経由でのアクセスおよび操作は、本サービス運用上の管理権限を持つ有資格者だけに制限しています。
    運用上の権限を持たない第三者はネットワーク経由で物理サーバにアクセスできないように運用しています。

2.5 物理サーバに対する対策(2/2)

FUJITSU

- 完全性
  - ウイルス感染抑止に向けた取組み

    クラウド基盤の運用作業に伴ってウイルス感染が起こらないよう、サービス開発および運用で使用する機器については、ウイルスチェック・脆弱性チェックなどのセキュリティチェックを実施しています。

    これによりウイルス感染による情報の改ざん、漏洩、クラウド基盤の破壊が起こらないようにしています。

※注意※

上記は、クラウド基盤に対する対策となります。利用者の仮想サーバなど、利用者が管理する リソースについては、

利用者自身でのウイルス対策などが別途必要です。

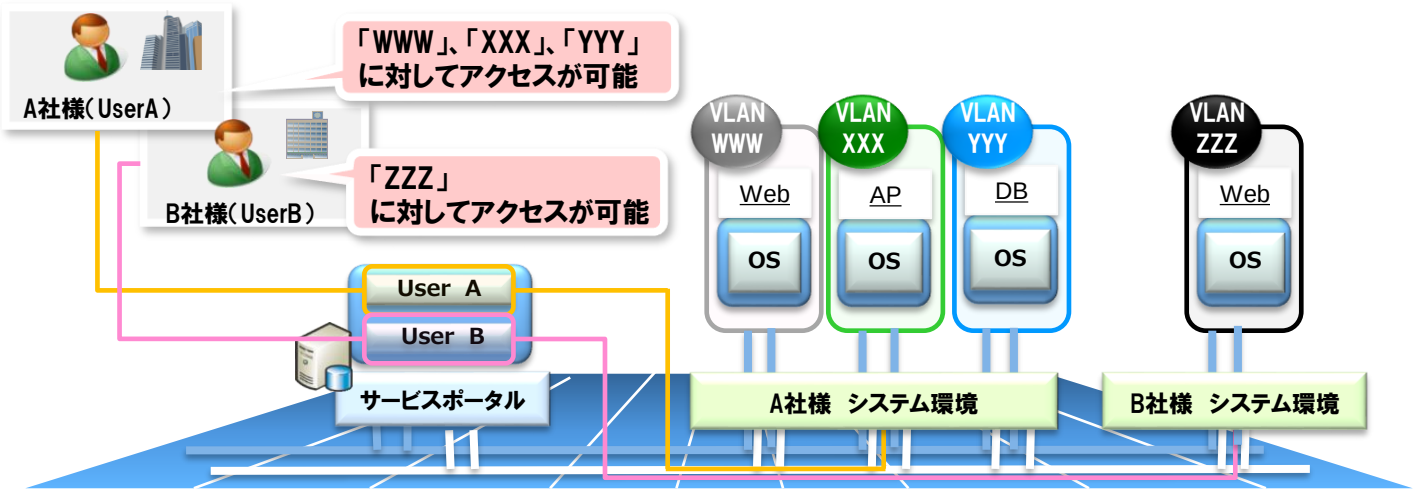
- 可用性
  - 物理サーバの電源二重化

    物理サーバは二系統の電源設備から受電することで、電源の二重化を行っています。
    UPS(無停電電源装置)による予備電源も具備しています。

2.6 仮想化基盤に対する対策(1/2)

- 機密性
  - VLANによるネットワークの区画化

IaaSでは、ネットワークや仮想サーバ環境を、複数のお客様で共用していただきますが、ご利用いただく環境は論理的に区分されており、サービスをご利用のお客様が、他のお客様からデータや通信内容を参照されることはありません。
※管理者用通信（監視等）と利用者用通信も、VLANにより分離しています。



2.6 仮想化基盤に対する対策(2/2)

- 完全性
  - 仮想化基盤に脆弱性が発見された場合の対応

    本サービスでは、仮想化基盤に関する脆弱性情報を、富士通内のセキュリティ専門部署が常時確認しています。

    本サービスで使用している仮想化基盤に脆弱性が見つかった場合には、本サービスの各担当部門に通知され、提供する機能・サービスへの影響を確認した後、速やかに修正対応の判断および修正適用を行う場合はその対応が行われます。

- 可用性
  - 仮想サーバのオートフェイルオーバ機能

    仮想サーバの稼働中にデータセンター内の物理サーバが故障などにより停止した場合、その物理サーバ上で稼働していた仮想サーバを、自動的に別の物理サーバに移動して稼働させることができます。

    オートスケール機能と併用できないため、本機能を利用するかどうかは利用者の判断となります。

FUJITSU

第３章　セキュアにご利用頂くために提供する機能

3.1 概要

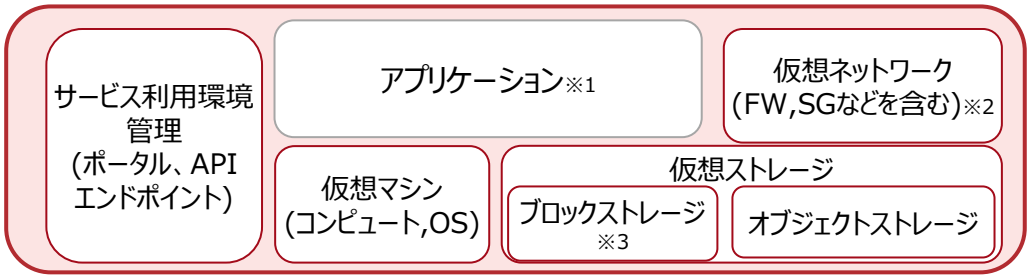
本サービスの利用者は、OSや、ミドルウェア、業務アプリケーションといった仮想サーバ環境や、仮想ストレージ、
仮想ネットワークの利用に関するセキュリティについては、利用者自身でセキュリティを確保する必要があります。
これには、本サービスが提供する機能やOSの機能、あるいは、サードパーティのソフトウェアなどを用います。

※システム全体のセキュリティを高めるためには、本サービスが提供している機能だけではなく、様々な機能を併用する必要がある点にご留意ください。
　従来、オンプレミス上(お客様自身の環境など)のシステムで行っていた対策と同等の検討が必要です。

３章では、本サービスをセキュアにご利用頂くために提供している機能をご紹介します。

なお、個々の機能詳細につきましては、 IaaS機能説明書などをご参照下さい。

また、データベースサービスやメール配信サービスなど個々のサービス固有の内容については、本章では記載していません。



※1:本サービスが提供するセキュリティ機能はないため、
　本章では記載しません。
※2:略語については以下のとおりです。
　FW:ファイアウォール
　SG:セキュリティグループ
※３:サーバにアタッチ(接続)して使用します。
　システムストレージ(システム領域用)
　増設ストレージ（データ領域用）

3.2 利用環境管理に関するセキュリティ機能

サービスの利用環境管理機能（ポータル、APIエンドポイント）に対するセキュリティ関連機能を以下に記載します。

サービス／機能名	概要	セキュリティ面での期待効果
利用者管理機能	サービスやリソースにアクセスできるユーザーを作成し、ユーザーの役割（ロール）に応じて、適切な操作権限を設定することができます。	ユーザーの作成や、ユーザーへの適切なロール割り当てによる操作権限の管理により、権限を持たない利用者によるリソースの削除などのシステム破壊を防止することができます。
証明書+パスワード認証	ポータルへのログインやAPI実行のためのトークン取得に際して、下記の２種類の認証方法を選択できます。 ①パスワード認証 ②証明書+パスワード認証	②の認証方法を選択した場合、2要素での認証であるため不正な利用者によるアクセスを抑止できます。

3.3 仮想マシン環境に関するセキュリティ機能

仮想マシン環境に対するセキュリティ関連機能を以下に記載します。

サービス／機能名	概要	セキュリティ面での期待効果
キーペア管理機能を用いた仮想サーバへのSSHログイン	仮想サーバ作成時にSSH通信を行うためのキーペアを登録、管理する機能を提供します。	仮想サーバ接続時にキーペアの鍵ファイルを用いることで、SSHによるサーバログイン、またはログイン情報の取得が可能です。IDやパスワードを利用せずに済むため、ブルートフォース攻撃(総当り攻撃)などによるサーバへのクラッキングのリスクを低減できます。
仮想マシンに対するアップデートサーバの提供	OSパッチの適用環境(WSUS/RHUI/yum) を提供します。	サービス内でOSの修正適用を行うことが可能です。
FUJITSU Hybrid IT Service FJcloud Trend Micro Cloud One - Workload Security オプション	仮想サーバに対して、以下の機能を提供します。 ・ウイルス対策機能 ・サーバに対するFirewall機能 ・ログ監視機能 ・サーバに対するIDS/IPS機能 ・Webレピュテーション機能 ・仮想サーバに対する変更管理機能	左記の機能により、仮想サーバに対する外部からのアタックを検知、防御することで仮想サーバからの情報流出や、サーバダウンのリスクを低減させることができます。

3.4 仮想ストレージに関するセキュリティ機能

仮想ストレージに対するセキュリティ関連機能を以下に記載します。

○ ブロックストレージ

サービス／機能名	概要	セキュリティ面での期待効果
スナップショット機能	利用中のブロックストレージに対して、スナップショットを作成する機能です。	外部からのアタックや利用者の過失によって、データ破損が生じた場合に、スナップショットからストレージディスクのデータを復旧することができます。
仮想サーバイメージの管理	作成済み仮想サーバのシステムストレージから、仮想サーバイメージを作成、管理する機能です。	外部からのアタックや利用者の過失によって、仮想サーバの再構築が必要になった場合に、あらかじめ取得していた仮想サーバイメージを用いて、サーバの新規作成を行うことができます。

○ オブジェクトストレージ

サービス／機能名	概要	セキュリティ面での期待効果
アクセスポリシーの設定	オブジェクトストレージに対して、読み取り／書き込みなどのアクセス権限を設定することが可能です。	正当にアクセスすべき権限を持たない第三者からのオブジェクトストレージへのデータアクセスを防止することができます。

3.5 仮想ネットワークに関するセキュリティ機能

仮想ネットワークに対するセキュリティ関連機能を以下に記載します。

サービス／機能名	概要	セキュリティ面での期待効果
IPsec VPN機能	オンプレミス環境との接続、またはリージョン間同士のシステム接続のために、IPsec VPNゲートウェイ機能を提供します。	利用者のIPsecゲートウェイと仮想ルータ間でIPsecを用いたVPN接続を行うことが可能になり、通信経路上での盗聴などの攻撃リスクを低減できます。
SSL-VPN機能	システム上に構築した仮想サーバにセキュアにログインして管理操作を行うために、SSL-VPN接続機能を提供します。	リモートアクセス端末と本サービスの間でSSL暗号化通信を用いたVPN接続を行うことが可能になり、通信経路上での第三者からの攻撃リスクを低減できます。
FUJITSU Hybrid IT Service FJcloud-O Digital enhanced EXchange	ホスティング環境やオンプレミス環境などのユーザー固有の環境と本サービスの利用者システムとを閉域接続するための機能を提供します。	閉域接続を行うことで、通信経路上での第三者からの攻撃リスクを低減できます。
ファイアーウォールサービス	仮想ルータに対して、パケットフィルタを行う機能を提供します。	仮想ルータで不正な通信を遮断することで、システムに対する第三者からの不正アクセスを防止することができます。
セキュリティグループ機能	仮想サーバに接続されたポートに対してパケットフィルタリングを行う機能を提供します。ルール設定をグルーピングして定義、設定することもできます。	仮想サーバに対する不正な通信を遮断することで、システムに対する第三者からの不正アクセスを防止することができます。

FUJITSU

4章　セキュリティ推進体制と取組み

4.1 セキュリティ推進体制（1/3）

○ 情報セキュリティへの組織的取組み

本サービスでは、クラウド情報セキュリティ基本方針および管理基準を基に、組織的に適切なセキュリティ教育を受けた運用者が、運用手順書に従い運用しています。

技術的対策だけでなく、サービス運用についても、運用端末、アクセス権を限定し、
運用者がアクセスする際のログを管理するなど、予防対策を講じることにより、問題が発生しないよう努めています。

また、万が一セキュリティ上の問題が発生した場合は、事象の識別、原因の究明を行い、被害を最小限かつ局所化に留めるように組織的に迅速な対応を実施します。

- **役員のコミットメント**
- **役割と体制**
- **情報管理区分**
- **コンプライアンス**
- **セキュリティ管理策**
- **脆弱性診断**
- **リスク評価**
- **モニタリングと監査**
- **サービスデスク　　など**

グローバルで共通の規程

ISO27000s,
NIST(*1), ENISA(*2)
Cloud Security Alliance の
ガイドライン等が
ベース

*1 National Institute of Standards and Technology
*2 European Network and Information Security Agency

4.1 セキュリティ推進体制（2/3）

FUJITSU

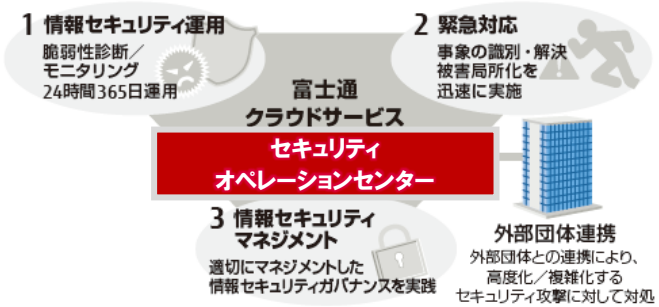
○ クラウドセキュリティ専門チームの設置

本サービスにおけるセキュリティの脅威（サイバーテロ、不正利用、情報漏洩など）に対して、予防および検知に努め、
万が一セキュリティ上の問題が発生した場合は迅速に対応するクラウドセキュリティ専門チーム「セキュリティオペレーションセンター（SOC）」の設置により、
トラステッド（高信頼）なサービスを提供しています。

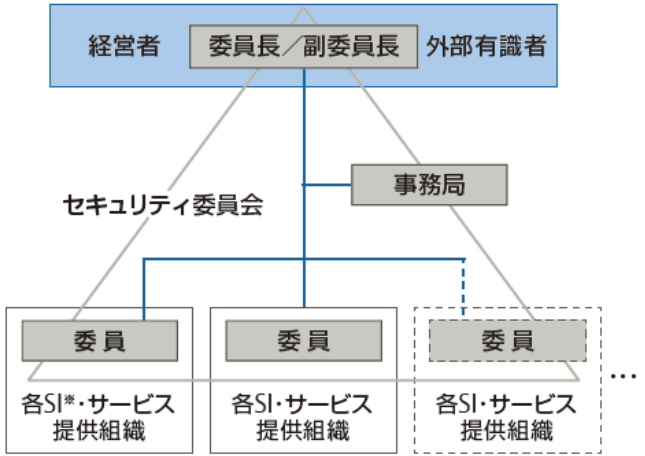
セキュリティオペレーションセンター（SOC）は、クラウドコンピューティングに特化した組織内セキュリティ専門チームです。外部からの様々な攻撃を水際で検知するモニタリングを24時間365日実施し、クラウド基盤をセキュリティの脅威より守ります。
万が一セキュリティ事故の発生を検知した際には、収束に向け迅速に対応を実施します。

また、社内にセキュリティ委員会を設け、本サービスにおける「人」「モノ」「情報」を適切にマネジメントし、情報セキュリティガバナンスを実践しています。

セキュリティオペレーションセンターの活動



セキュリティ委員会体制



〔※〕SI：システムインテグレーション

4.1 セキュリティ推進体制（3/3）

FUJITSU

○ 社外セキュリティインシデントチームとの連携

社外のセキュリティインシデント対応チームと連携することで、高度化、複雑化するセキュリティ攻撃に対してグローバルな観点で適切に対処します。

・FIRST（Forum of Incident Response and Security Teams）

セキュリティインシデントの情報の収集、提供、共有をサポート。95の国と地域のCSIRTがメンバーとして登録され、
その数は500以上に上る。米国Cisco, intel, Microsoft, IBM, HPのほか日本からも楽天、KDDI、RICOH、Panasonic などが加盟。

・JPCERT/CC (JPCERTコーディネーションセンター)

インターネットを介して発生するコンピューターセキュリティに関連する事象の情報を収集し、インシデント対応の支援、
コンピュータセキュリティ関連情報の発信などを行う組織。日本の代表的なCSIRTである。

・日本CSIRT協議会（CSIRT: Computer Security Incident Response Team）

コンピュータセキュリティインシデントへの迅速な課題解決のために、加盟チームの緊密な連携体制の実現目指す活動を行う。
日本アイ・ビー・エム、日立製作所、楽天、ヤフー、NRIセキュアテクノロジーズ、 NECグループ、インターネットイニシアティブなどが参加。

※上記の加盟数、団体等は2020年2月時点の情報です

4.2 サービス基盤のセキュリティ運用(1/4)

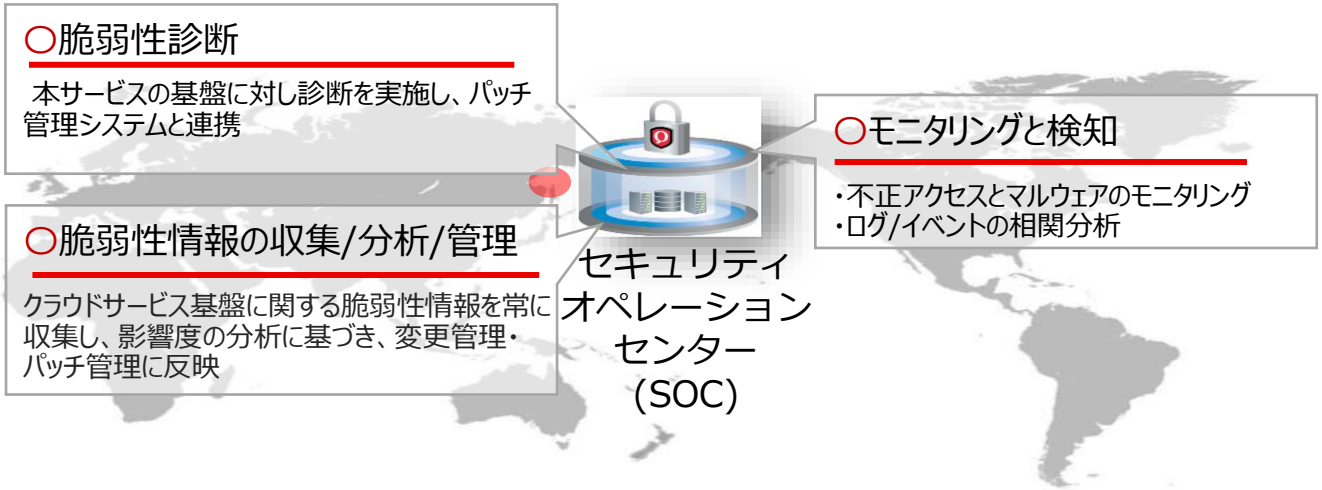
FUJITSU

○　脆弱性診断・モニタリングと検知

セキュリティオペレーションセンター（SOC）にてクラウド基盤に対するモニタリングなどの情報セキュリティ対策を実施し、24時間365日体制で運用しています。

・脆弱性診断
クラウド基盤に対し脆弱性診断を行い、問題があった場合は関連部署と検討・協議し、セキュリティパッチ管理システムと連携のうえ対応を実施します。

・モニタリングと検知
24時間365日不正アクセスとマルウェアのモニタリング、ログ/イベントの相関分析などを行っています。何か問題があれば関連部署と情報共有し
連携して迅速に対応します。



4.2 サービス基盤のセキュリティ運用(2/4)

FUJITSU

○ 脆弱性情報の収集・分析・管理のプロセスを確立

クラウド基盤に関する脆弱性情報を常に収集し、専任チーム「富士通クラウドCERT」による分析を実施、インパクト（影響度）に応じたトリアージ(影響度と緊急度からの優先度付け)を行い、変更管理・パッチ管理に反映するプロセスを確立しています。

変更管理、パッチ管理に基づきクラウド基盤への脆弱性対策を実施することにより、
利用者にトラステッド（高信頼）なパブリッククラウドサービスを提供しています。

脆弱性情報の収集

国内/国外の約100サイトのフィード収集

「JPCERT/CC早期警戒情報」の個別入手

JPCERT/CCのVRDA*（ヴァーダ）フィード収集

* Vulnerability Response Decision Assistance
（脆弱性対応意思決定支援システム）

インパクト分析

分析プロセス
- トリアージ（インパクト別）
- プロダクトの該当/非該当の詳細判定

分析スキーム
- 専任のリスクコントロールチームが担当

変更管理・パッチ管理

CAB*にて最終決定

セキュリティ・サブCABにて優先順位検討

* Change Advisory Board
（変更諮問委員会）

4.2 サービス基盤のセキュリティ運用(3/4)

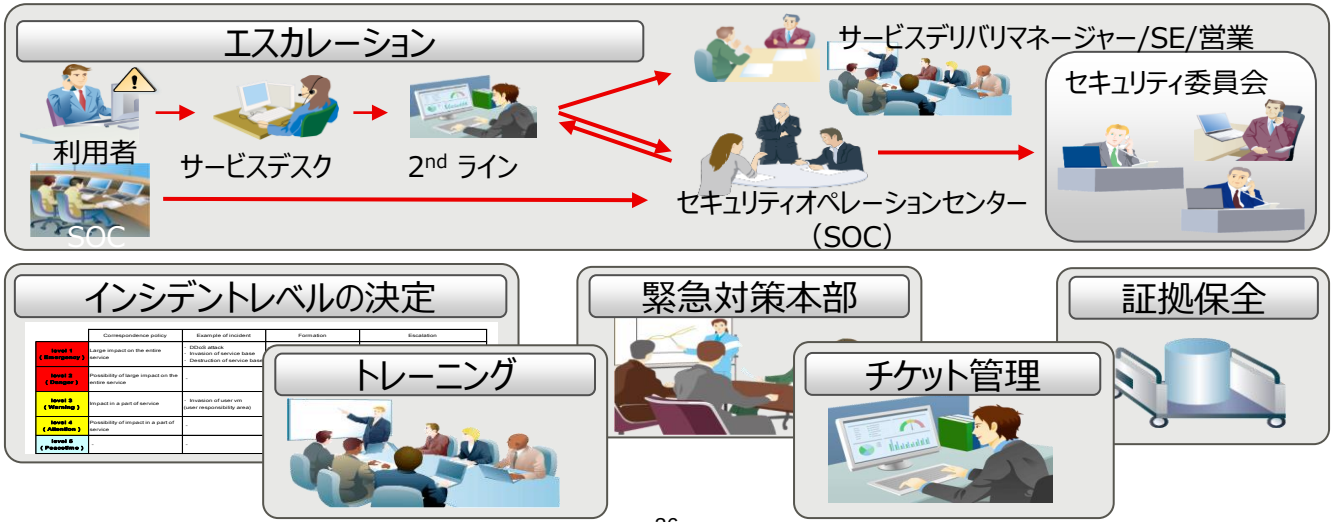
FUJITSU

○ 迅速・確実なインシデントマネジメントの実施

本サービスでは、セキュリティインシデント発生時の対応プロセスを定めており、万が一にセキュリティインシデントが
発生した際には、事象の識別・解決・被害局所化を迅速かつ確実に実施します。

クラウド基盤に関する（利用者システム固有の問題を除く）セキュリティインシデントの発生を検知した場合、専門チームにエスカレーションされ、インシデントレベルの
トリアージ(影響度と緊急度からの優先度付け)を行い、
事象の確認、インパクト（影響度）を判断、必要に応じて緊急対策本部を設置し対応いたします。

また、万が一セキュリティインシデントが発生した場合に備え、迅速に行動ができるよう定期的にトレーニングを実施し、
関連部署との連携確認、証拠保存などのオペレーション訓練を行っています。



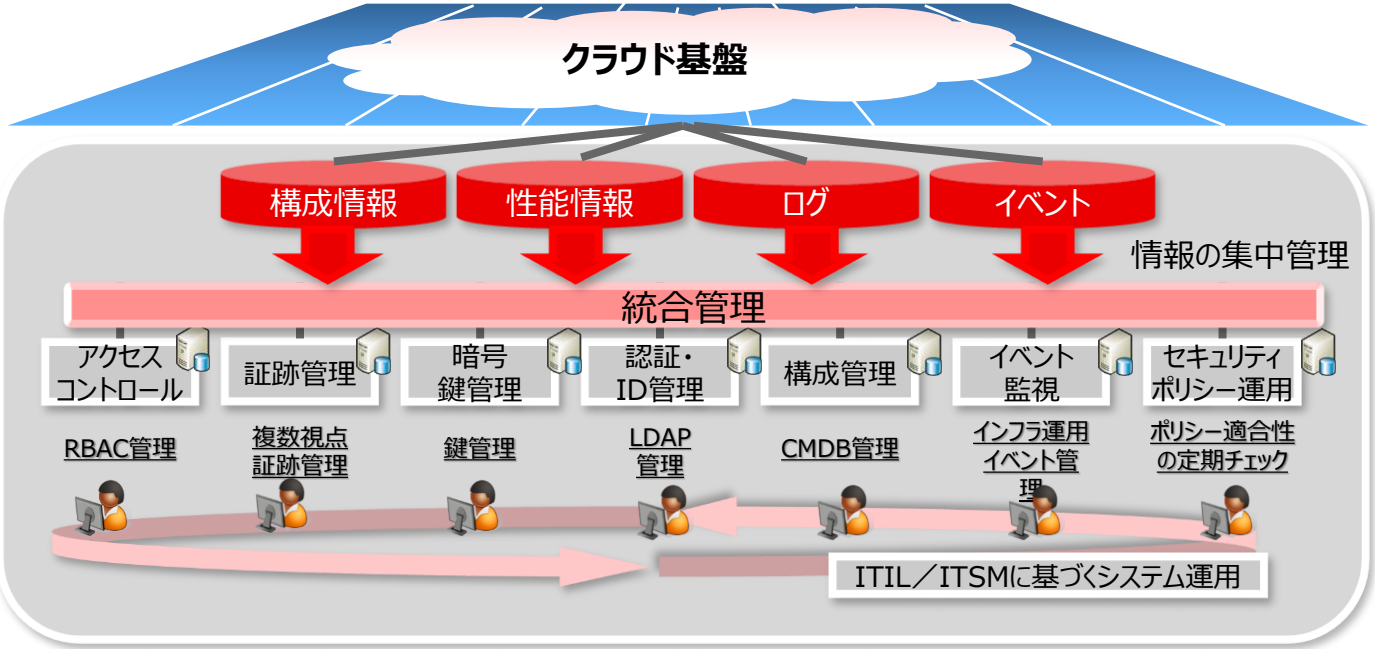
4.2 サービス基盤のセキュリティ運用(4/4)

FUJITSU

○ 情報の集中管理

クラウド基盤の「構成情報」「性能情報」「ログ」「イベント」を統合管理することにより、課題を可視化し、課題への対処を迅速に対応できる体制を整えています。

クラウド基盤に関わる各機器（物理サーバ、ネットワーク、ストレージなど）のリソース状況、ネットワーク利用状況、APIの受付状況などを常に監視しサービスを維持するためのキャパシティ管理、ネットワーク管理を行っています。
クラウド基盤に対する監視を実施しており、利用者個別のリソースの監視は実施していません。



FUJITSU

5章　各リージョンに関する情報

5.1 認証・規格への対応状況

- 認証・規格への対応状況は以下のリンクをご参照ください。

FUJITSU Hybrid IT Service FJcloud-O / FJcloud-ベアメタル　認証取得状況

FJcloud-O： https://jp.fujitsu.com/solutions/cloud/fjcloud/-o/document/authenticate.html

FJcloud-ベアメタル： https://jp.fujitsu.com/solutions/cloud/fjcloud/-baremetal/authenticate/

5.2 各リージョンの法制度

FUJITSU

○ 法制度

本サービスでは、利用規約に準拠法および専属的合意管轄裁判所を定めています。

利用者が、本サービス上に保管したデータについても同様に法令等の遵守が求められ、利用者自身での管理が必要となります。
本サービスでは、利用者のデータは等しく扱い、内容については関知しておりません。

法令、裁判所の命令その他法的手段により、第三者へのデータ開示を強制された場合に、法的に開示可能な範囲で、本サービスにおいて定められたプロセスに従い判断を行います。

付録.用語説明（1/2）

用語	説明
アベイラビリティゾーン(AZ)	データセンター設備やサービス提供用設備などの物理的な施設を共有する単位。
仮想サーバイメージ(イメージ)	配備済の仮想サーバより、固有情報を削除した雛形を用意し容易に仮想サーバの複製が行える機能。
APIエンドポイント	クライアントが API にアクセスするための通信の接続先。
オートスケール	システム負荷などの条件に従って、仮想サーバの増減を自動的に制御する機能。
オートフェイルオーバ	サービス提供環境でハードウェアトラブルなどが生じた場合、自動的に他のハードウェアでサービスを再開する仕組み。
オブジェクトストレージ	オブジェクト(コンテンツとメタデータからなる)単位で分割保存するストレージ。
外部ネットワーク	インターネットに接続するために本サービスIaaS側で用意したネットワーク。
仮想ネットワーク	仮想サーバなどのリソースが通信するための仮想的なネットワーク。サブネットに対応して作られる。
仮想ルータ	外部ネットワークとネットワーク、またはネットワーク同士を接続する機能。
キーペア	仮想サーバへSSHでログインする場合や、Windowsのランダムパスワードを暗号化するために使われる公開鍵と秘密鍵の組み合わせ。仮想サーバには公開鍵のみが登録される。
CMDB	構成管理データベース。サービス提供に必要な全てのコンポーネントに関する情報(構成管理)の管理を行うデータベース。
サブネット	ネットワークの論理分割単位。配備されるリソースに対してプライベートIPアドレスの管理、DHCP機能、ルーティング管理などを提供します。
スナップショット	ブロックストレージの状態をあるタイミングで抜き出したもので、バックアップなどに利用することが可能。
セキュリティグループ	仮想サーバに接続されたポートに対してパケットフィルタリングを行うルールをグルーピングする機能。
ティア	JDCC（Japan Data Center Council、日本データセンター協会）が定めたデータセンターファシリティスタンダード。ティア1からティア4の4段階に分類し、ティア4が最上位となる。
内部ネットワーク	インターネットに接続されていないネットワーク。
ファイアーウォールサービス(FW)	仮想ルーターに対するパケットフィルタリングルール。
ブロックストレージ	システムストレージ、増設ストレージとして利用可能なデバイス。

付録.用語説明（2/2）

用語	説明
ポート	仮想サーバなどリソースをネットワークに接続するため、IPアドレスとの関連付けを行うネットワークインターフェース。
リージョン	各国または国内における東西、南北など地域的に隔離された単位。
RBAC	ロールベースアクセス制御。ロール（役割）によりポリシーを柔軟なアクセス制御が可能。

FUJITSU

Thank you