FUJITSU Hybrid IT Service
FJcloud-O / FJcloud-ベアメタル
セキュリティホワイトペーパー

2020/10/30

富士通株式会社

目次

はじめに

FUJITSU Hybrid IT Service FJcloud-O / FJcloud-ベアメタル（以下、FJcloud-O / FJcloud-ベアメタルと記す）とは、オープンテクノロジーをベースに当社の知見やノウハウを「Knowledge」として蓄積させ、お客様の開発／運用の効率性を向上するクラウドサービスです。お客様やパートナー様の業務ノウハウ、オープン技術を取り込み、『スピーディな機能拡張』を実現することで、ビジネスの加速に貢献します。

「FUJITSU Hybrid IT Service FJcloud-O / FJcloud-ベアメタルセキュリティホワイトペーパー」（以下、本書）では、FJcloud-O / FJcloud-ベアメタルで提供する情報セキュリティ対策について説明します。

本書について

- 本書は、富士通が情報提供のみを目的に作成したものです。
- 本書は、作成した時点における富士通の見解を反映したものです。予告なく変更されることがあります。
- 本書のいかなる内容も富士通の保証、表明、義務、確約等を意味するものでなく、本書の内容の正確性、特定の目的への適合性を含め、富士通は本書に関するいかなる保証も行いません。また、本書の利用により生じたいかなる状況についても、その理由の如何を問わず、一切の責任をおいません。
- FJcloud-O / FJcloud-ベアメタルを利用するお客様との契約条件は「FUJITSU Hybrid IT Service FJcloud 利用規約」等に定める通りであり、本書はその一部にはなりません。
- 本書の内容の全部または一部を無断転記することを禁じます。
- 本書に記載されている会社名、製品名、などは、それぞれ各社の商標、登録商標、製品名です。

輸出管理規制

- 本ドキュメントを輸出また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関連法規等をご確認のうえ、必要な手続きをおとりください。

1　クラウドサービスのセキュリティ

1.1 クラウドサービスの動向

昨今、オンプレミスの ICT システムとクラウドサービスを組み合わせたハイブリッド IT 環境での運用や、複数のクラウドサービスを組み合わせたマルチクラウドの利用など、クラウド基盤の活用が広がっています。また、日本政府もクラウド・バイ・デフォルト原則を掲げ、政府の ICT システムにおけるクラウドサービスの利用を拡大しています。これは、ICT システムを単にクラウドに移行するだけでなく、IoT や BigData、また AI を活用し、共創によるモノづくりでビジネスの拡大と業務の更なる効率化、そして利便性を向上するために、データやサービスの連携や活用が容易なクラウドサービスの利用が欠かせないということが理由の一つです。

1.2 情報セキュリティの動向

ICT システムにおける情報セキュリティの問題は、より複雑になっています。サイバー攻撃が多様化・巧妙化する一方で、セキュリティに対応する人材の不足が指摘されています。IPA[1]「IT 人材白書 2018」（調査年：2017 年度）によると 3 割強の IT 企業が情報セキュリティの専門技術者を確保できていないと回答しています。また、ICT システムに求められるセキュリティが、防御や検知といったインシデントが発生するリスクを軽減するだけでなく、被害を局所化するための分析や対処、そしてサイバー攻撃への耐性を強化するなど、幅広く求められるようになってきています。このため、後付けでのセキュリティ対策では対応が難しくなっています。こうした状況に対応するため、ICT システムの企画・設計段階からセキュリティ確保を考慮したセキュリティ・バイ・デザインの取り組みが求められています。

また、共創の場を支えるクラウドサービスを誰もが安心して、かつ安全に利用するため、クラウドサービスに特化したセキュリティ評価を行う動きも出ています。国際規格である ISO/IEC27017 による認証や各種の基準、またはガイドラインに基づく評価と対応状況の公開などの動きがあります。

1.3 クラウドサービスに求められるセキュリティ

こうした状況を背景に、私たちクラウドサービスプロバイダにおけるセキュリティ対応が重要と認識しています。サービスプロバイダとして、セキュリティ専門家およびセキュリティが分かる開発者や運用者といった人材を確保し、ICT システムの設計、開発、そして運用においてクラウドサービス基盤のセキュリティ対応を実践し、一定水準のセキュリティ対応を行うことで、お客様に安心してクラウドサービスをご利用いただくことができます。また、例えば権限設定の機能などセキュリティ機能をサービスプロバイダがお客様に提供することで、お客様のセキュリティ対応をお手伝いすることが出来ます。

ここで、クラウドサービスの利用における情報セキュリティの特徴を 2 つの視点で整理してみます。

まず、ICT システムの構成要素に対するセキュリティの役割および責任という点に特徴があります。一般に、クラウドサービスを利用してシステムを運用することで、お客様自身の環境でシステムを運用する場合と比べ、お客様自身で管理しなければならない範囲は小さくなります。代わりに、管理の一部を私たちクラウドサービスプロバイダが実施します。

インフラストラクチャアズアサービス（IaaS）のクラウドサービス区分を例に、一般的な役割分担を表 1-1 に示します。この表を見ると分かりますが、クラウドサービスの利用においてはセキュリティ対策の一部を私たちクラウドサービスプロバイダが実施いたします。お客様に、この役割と責任範囲をご理解いただくことが大切であると私たちは考えます。

[1] IPA(独立行政法人 情報処理推進機構)

表 1-1 IaaS におけるシステムの構成要素とセキュリティ対応の役割および責任

<table>
<tr><th colspan="2">構成要素</th><th>セキュリティの役割</th><th>責任</th></tr>
<tr><td rowspan="4">論理レイヤ</td><td>データ、業務アプリケーション</td><td rowspan="3">仮想サーバ環境の維持と管理</td><td rowspan="3">利用者</td></tr>
<tr><td>ミドルウェア</td></tr>
<tr><td>オペレーションシステム</td></tr>
<tr><td>仮想マシン/仮想プラットフォーム
/管理コンソール</td><td>仮想化基盤および
サービス基盤の管理</td><td rowspan="3">クラウドサービス
プロバイダ</td></tr>
<tr><td rowspan="2">物理レイヤ</td><td>物理マシン</td><td>物理的な機器の管理
(サーバ、ネットワーク機器など)</td></tr>
<tr><td>ファシリティ</td><td>機器が設置される施設の管理
(データセンターなど)</td></tr>
</table>

また、クラウドサービスの利用を考慮した情報セキュリティ管理の点も大切になります。組織において情報セキュリティを維持管理するためには、組織の方針に従って必要なセキュリティレベルを決め、計画に沿って人材を含むリソースの確保や ICT システムの開発と運用を行います。クラウドサービスを利用する場合には、従来の情報セキュリティ管理の実施方法を変える、または一部をクラウドサービスプロバイダに委託するなどの対応が必要となります。表 1-2 に概要を整理しました。

表 1-2 クラウドサービスを利用する場合の情報セキュリティマネジメントの考え方

<table>
<tr><th>区分</th><th>実施の方法</th><th>対応項目の例</th></tr>
<tr><td rowspan="2">1) 従来と同じセキュリティ対応</td><td>a) 従来と同じ</td><td>・ セキュリティ基本方針
・ セキュリティ管理
・ アクセス制御および暗号化※
・ 運用管理※
・ 通信のセキュリティ※
・ システム開発と保守
・ 供給者との関係※
・ セキュリティインシデント※
・ 遵守※
※ 一部、b)または c)に含まれる項目</td></tr>
<tr><td>b) (クラウドサービスを利用する場合には)実施方法が異なる</td><td>・ ログの取得および監視
・ 運用セキュリティ
・ バックアップ
・ ネットワークセキュリティ管理</td></tr>
<tr><td>2) クラウドサービス固有のセキュリティ対応</td><td>c) (クラウドサービスを利用する場合は)新たに対応が必要</td><td>・ 責任分解の明確化
・ テナント間の分離(データライフサイクルマネジメント、アクセスコントロールなど)</td></tr>
</table>

例えば、1)-b)項に含まれるログの取得および監視については、従来はお客様が自身で実施していました。しかし、クラウドサービスを利用する際には、共有リソースに関するログの取得および監視を私たちクラウドサービスプロバイダが実施しています。一方で、お客様の利用環境における仮想リソースやお客様環境で実行するアプリケーションの監視については、モニタリング用の監視サービスを提供してお客様が実施できる仕組みを提供しています。また、クラウドサービスを利用する場合には、プライベートなネットワーク領域とパブリックなネットワーク領域との境界が従来と異なります。それぞれの境界でフィルタリングや通信の監視などネットワークセキュリティ管理を行う必要があります。ログの取得と同様に、ネットワークセキュリティ管理においても共有リソースのセキュリティ対応を私たちクラウドサービスプロバイダが実施します。詳細は 5.4 節 通信のセキュリティを参照してください。

2)-c)項についてはクラウドサービスで対応が必要となる項目です。私たちクラウドサービスプロバイダはクラウドサービス基盤でこれらの対応を行っています。例えば、クラウドサービスでは物理的および仮想的なリソースを共有することから、テナント間の分離を実現し維持管理することが重要です。他の利用者やクラウドサービスプロバイダとのアクセス権限の分離などを行います。詳細は、5.2 節 物理および環境的セキュリティ、および 5.3 節 アクセス制御および暗号化を参照してください。

1.4 クラウドサービスにおけるセキュリティの考え方

FJcloud-O / FJcloud-ベアメタルは、クラウドサービスプロバイダとしてクラウドサービス基盤および仮想基盤、そして物理レイヤのセキュリティ対応に取り組むことで、お客様が安心してご利用いただけるクラウドサービスです。

本書 2 章以降では、富士通がクラウドサービスプロバイダとして取り組むセキュリティ対応をご説明します。お客様と富士通が情報セキュリティの役割と責任を適切に分担しセキュリティ対応に取り組むことが安全なクラウドサービスの利用を実現する上で大切であると私たちは考えます。お客様に富士通の対応をご理解いただくため、情報提供に努めていきます。

2　FUJITSU Hybrid IT Service FJcloud-O / FJcloud-ベアメタルのセキュリティ基本方針

<ISO/IEC 27017 5.1.1>

富士通の情報セキュリティに関する基本的な考え方は、富士通グループの理念・指針である「FUJITSU Way」に基づいています。

また、富士通グループでは、海外の関連会社を含む全ての富士通グループ向けの統一的な情報セキュリティポリシーである「富士通グループ情報セキュリティ基本方針」（詳細はこちら）を定め、この方針に従って関連規程を整備して、情報セキュリティを実施しています。

さらにリスクマネジメントおよびコンプライアンスにかかわる最高決定機関として、取締役会に直属する「リスク・コンプライアンス委員会」を設置しています。リスク・コンプライアンス委員会を中心として、これらのリスクを認識および評価したうえで、リスクの回避、軽減、移転および保有を判断および実行し、万が一問題が発生した場合には影響の極小化に努めています。

FJcloud-O / FJcloud-ベアメタルおよびそれを運営する組織では、「富士通グループ情報セキュリティ基本方針」に従い、情報セキュリティ実施基準、運営組織の情報セキュリティ基本方針および FJcloud-O / FJcloud-ベアメタルの情報セキュリティポリシーなどの方針群を内部文書で定めており、これに基づいて情報セキュリティ対策（機能面、運用面）を適切に実施し、FJcloud-O / FJcloud-ベアメタルを提供・運営しています。

お客様からお預かりした大切な情報を適切に取り扱い、お客様の権利および利益を保護します。FJcloud-O / FJcloud-ベアメタルのサービスを安定的に提供することにより、その社会的機能を維持します。

また、情報セキュリティマネジメントシステム（ISMS）の規格である「ISO/IEC 27001:2013(JIS Q 27001:2014)」や「ISO/IEC 27017:2015(JIS　Q 27017:2016)に基づく ISMS クラウドセキュリティ認証」の第三者評価認証制度による認証の取得を始めとして、FISC 安全対策基準を含めた SOC2 保証報告書、PCI DSS における準拠証明書（AOC）などを取得または受領し、外部の客観的なチェック機構も積極的に活用しています。

詳細な情報をご希望の場合には、富士通のお客様を担当する営業またはヘルプデスクへお問い合わせください。ただし、お問い合わせの内容によっては、開示をお断りする場合もあります。あらかじめご了承下さい。

3　FUJITSU Hybrid IT Service FJcloud-O / FJcloud-ベアメタルのセキュリティの枠組み

3.1 セキュリティの役割及び責任

<ISO/IEC 27017 6.1.1>

<ISO/IEC 27017 6.1.3>

FJcloud-O / FJcloud-ベアメタルの利用規約や各サービス仕様書等で契約やサービス内容及び、お客様と各サービスを提供する富士通の責任範囲を示しています。以下に IaaS におけるお客様と FJcloud-O を提供する富士通の責任範囲を示します。PaaS については各 PaaS のサービス仕様書、FJcloud-ベアメタルについては FJcloud-ベアメタルのサービス仕様書を参照してください。

FJcloud-O IaaS は、仮想化されたコンピューティング資源及び，コンポーネントをサービスとしてポータル及び API を通じて提供し、「FJcloud-O を構成するための物理的設備（物理機器を配置するファシリティ（データセンター）や物理機器）からポータル及び API までのコンポーネント（仮想化基盤を含む各種 IaaS サービス管理を構成するコンポーネント）とサービス運用」（以下、「FJcloud-O サービスと記す」）に責任を有しています。

ポータルや API を通じて作成したサーバやインストールした OS、MW やアプリケーション、保管したデータなどの「リソースやコンポーネント」は、利用者が任意に変更・削除できます。お客様の利用環境内のリソースについては、お客様の責任となります。

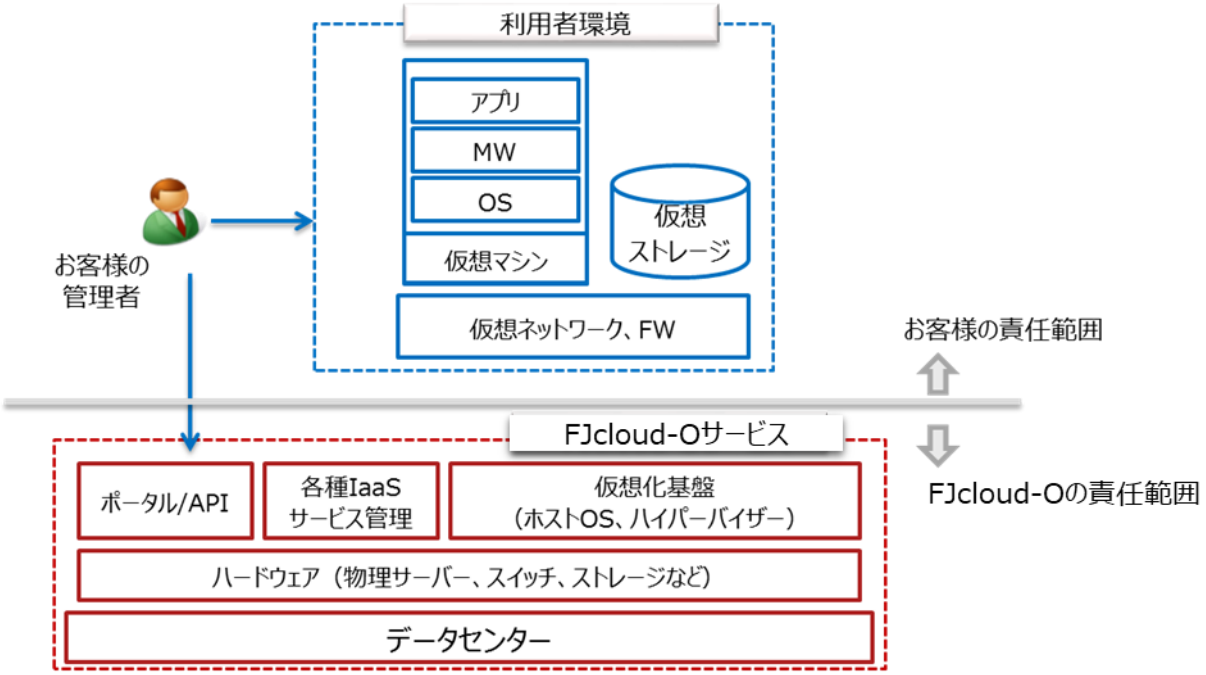

図 3-1 FJcloud-O IaaS における責任範囲

3.2 クラウドコンピューティング環境における役割

<ISO/IEC 27017 CLD.6.3.1>

FJcloud-O / FJcloud-ベアメタルのサービス提供において様々な情報セキュリティリスクが存在します。万が一セキュリティ上の問題が発生した場合、事象の識別、原因の究明を行い、被害を最小限かつ局所に留めるように、セキュリティリスクに組織的に迅速な対応を実施します。

セキュリティの脅威（サイバーテロ、不正利用、情報漏えいなど）に対して予防および検知に努め、セキュリティ上の問題が発生した場合に備え、迅速に対応する組織内セキュリティ専門チーム「SOC」を設置しています。SOC は組織内の開発・運用部隊とは独立した第三者的立場の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、FJcloud-O / FJcloud-ベアメタルサービス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。なお、社会的影響およびお客様への影響が重大な場合、富士通のリスク・コンプライアンス委員会にエスカレーションし、その委員会で規定されたルールおよび手順に則って判断および対策・実行し、影響の極小化に努めています。

4　FUJITSU Hybrid IT Service FJcloud-O / FJcloud-ベアメタルセキュリティ管理

4.1 情報セキュリティの意識向上、教育及び訓練

<ISO/IEC 27017 7.2.2>

4.1.1 従業員の管理

富士通グループにおいて社員は最大の財産であり、富士通グループは社員の多様性を尊重し、社員が仕事を通じてその能力や専門性を高め、自己の成長を実現できるよう支援することを、FUJITSU Way の企業指針として定めています。

また、富士通グループでは、FUJITSU Way に基づき、従業員の管理を徹底しています。入社後も富士通の情報セキュリティ基本方針に基づく教育と啓蒙を実施しています。また、定期的に作業環境をチェックすることで、情報セキュリティに対する問題意識の形骸化を防止しています。

4.1.2 情報セキュリティに対する意識啓発

富士通グループでは、情報漏えいを防ぐために規程類を従業員に周知するだけでなく、役員および、派遣社員を含む全従業員に対して情報管理に関する教育を毎年実施し、情報管理の意識を徹底しています。また、さまざまなパートナー企業と連携し、入門・基礎技術に関する教育からクラウド専門の教育までさまざま教育コースを実施しています。併せて、社内のセキュリティ資格制度を設け、認定することでより高いスキルを持つ要員を育成しています。

FJcloud-O / FJcloud-ベアメタルに従事する要員に対しては、各サービスを開発・運用する上で必要となる情報セキュリティ教育を年 1 回実施し、スキル向上を図っています。

4.1.3 訓練

FJcloud-O / FJcloud-ベアメタルの安全かつ安定した運用を提供するために、障害、事故、災害に備えて、定期的にトラブル対応、インシデント対応、事業継続や防災訓練を実施しています。

4.2 情報資産管理

<ISO/IEC 27017 8.1.1>

<ISO/IEC 27017 8.2.2>

FJcloud-O / FJcloud-ベアメタルを利用するお客様の情報資産と FJcloud-O サービス / FJcloud-ベアメタルサービスの提供に必要な情報資産とを明確に分離しています。お客様の情報資産については、各サービスを利用するお客様システムのライフサイクルに渡って、サービスのポータル及び API 等によりお客様環境上に保管される情報資産の管理をインターネット経由で実施することができます。詳しくは利用規約、各サービス仕様書等を参照してください。また、各サービスの運用者がお客様の情報資産にアクセスすることはありません。

FJcloud-O / FJcloud-ベアメタルの提供に必要な情報資産については、不正アクセスや盗難などによる情報漏えいを防止するために、社内ルールに基づいて情報資産を重要度に応じて分類し、ラベル付けを行うと共に、ストレージや通信の暗号化も含めて適切に管理しています。

4.3 お客様の情報資産の削除

<ISO/IEC 27017 CLD.8.1.5>

サービス解約時、各サービス設備内のお客様の情報資産は、お客様の責任で削除して頂く必要があります。解約手続きが完了した以降、お客様が解約前に利用していたリソースが残存している場合には、利用規約に基づいて富士通にて削除いたします。

5　FUJITSU Hybrid IT Service FJcloud-O / FJcloud-ベアメタルにおけるセキュリティ対策

5.1 概要

FJcloud-O / FJcloud-ベアメタルでは情報セキュリティ対策の基本として多層防御の考え方を取り入れ、さまざまな対策を組み合わせて防御することで、「インターネットとの境界に防御壁を配備し攻撃を防ぐ」、「多重に検知機能を配置し攻撃成功を早期に発見する」、「侵入されたとしても防御壁を多重に配備し被害を最小限に抑える」の実現に継続的に取り組んでいます。

また、情報システムマネジメントシステム（ISMS）の規格である「ISO/IEC 27001:2013(JIS Q 27001:2014)」や「ISO/IEC 27017:2015(JIS Q 27017:2016)に基づくISMS クラウドセキュリティ認証」を始めとする客観的な評価（第三者評価制度、監査会社など）による認証、監査の保証報告などを積極的かつ継続して取得することで、セキュアなサービス提供を維持しています。

5.2 物理および環境的セキュリティ

5.2.1 物理セキュリティを保つべき領域

<ISO/IEC 27001 9.1.1>

FJcloud-O / FJcloud-ベアメタルのサービスを提供するデータセンターやサービスを運用する拠点では、物理的なセキュリティ境界と各区画の入室資格者区分を明確すると共に、ルールを定めて適切に管理を行っています。

例えば、東日本リージョンのデータセンターでは、以下のような技術や運用によりクラウドサービスの設備を保護しています。

- ・外周赤外線センサー監視　：データセンターの外周に赤外線センサーを設置し、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つけられる運用体制
- ・高精度監視　：高機能カメラにより昼夜を問わず高精度な監視を実施、また、モーション検知により異常状態を検知
- ・24 時間有人監視　：警備員が 24 時間待機および待機。警察署と共同で年 2 回防犯訓練を実施
- ・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
- ・セキュリティエリアの設定　：センター内に複数のセキュリティエリアを設定し、入館者は入室資格に応じた区画のみ立入り可能
- ・ラックセキュリティ　：手のひら静脈認証でラック施錠／解鍵管理、ラックハンドルは電気錠化
- ・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
- ・サーバ室入室時の共連れ防止：FeliCa カード、動線カメラ、生体認証を連動させ、共連れを防止

5.2.2 装置のセキュリティを保った処分または再利用

<ISO/IEC 27017 11.2.7>

装置の移動、修理、廃棄の場合には、円滑、確実かつ安全に実施するため、廃棄または再利用する業者が当社の定めたルール・基準を満たしているかの確認をするなど、不正防止、機密保護対策を含めた計画・ルール・手順を策定し、適切に実施することで情報漏えい対策に取り組んでいます。

5.3 アクセス制御および暗号化

5.3.1 アクセス制御方針

<ISO/IEC 27017 9.1.1>

FJcloud-O / FJcloud-ベアメタルにおける情報セキュリティに関するポリシーを定め、これに基づいて適切なアクセス管理を実施しています。

また、お客様のサービス利用ライフサイクル全てのシーンにおいても、適切なアクセス制御を実施しています。アクセス制御のポイントについて 5.3.2～5.3.4 項で説明します。

5.3.2 ネットワーク及びネットワークサービスへのアクセス

<ISO/IEC 27017 9.1.2>

FJcloud-O / FJcloud-ベアメタルでは、お客様のリソースとサービス管理のための領域とをネットワークを含めて分離しています。また、お客様自身がお客様のリソースやそのアクセスが可能なネットワークを含め分離する機能をポータル及び API より提供しています。

5.3.3 お客様によるアクセス

<ISO/IEC 27017 9.2.1>
<ISO/IEC 27017 9.2.2>
<ISO/IEC 27017 9.2.4>

FJcloud-O / FJcloud-ベアメタルでは、お客様の仮想マシン、仮想ストレージ、仮想ネットワークなどのお客様リソースの配備や構成設定、稼働状況の確認などの管理を行うサービスポータルを利用するための利用者登録及び削除機能を提供しています。

お客様に割り当てられた ID およびパスワードについてはお客様の責任で管理をお願いします。

なお、繰り返し行われるログインの試行に対して一定の試行回数で ID をロックアウトする機能や、定期的なパスワード更新など安全にアクセス頂くための機能を提供しています。詳しくは、「FJCS ポータルユーザーズガイド」を参照してください。

FJcloud-O / FJcloud-ベアメタルを利用するお客様の契約者は、各サービスリソースの利用権限を管理することができます。ユーザーやグループなどの管理単位ごとに、契約者、管理者、運用者などのロールを設定することができます。詳しくは、「FUJITSU Hybrid IT Service FJcloud-O IaaS サービス仕様書」を参照してください。

5.3.4 FUJITSU Hybrid IT Service FJcloud-O / FJcloud-ベアメタルサービス基盤へのアクセス

<ISO/IEC 27017 9.2.4>
<ISO/IEC 27017 9.4.1>
<ISO/IEC 27001 9.4.3>
<ISO/IEC 27017 9.4.4>

FJcloud-O / FJcloud-ベアメタルでは、サービス提供に携わる要員の役割に応じた権限設定を行うと共に、情報、システムやアプリケーションへの認可されていないアクセスを防止するために、情報、システムやアプリケーションごとに管理手順を定めて適切に実施しています。また、情報、システムやアプリケーションにアクセスした各種ログを一定期間保存し、不正防止やインシデントの発生を防止しています。

また、サービス提供に携わる要員が各サービス基盤にアクセスするためのログイン手順やパスワード管理に対するセキュリティに配慮したポリシーと手順を定めて、適切な管理を実施しています。

さらにサービス提供基盤に対する操作のための手順・各種ツール、使用ルールを定めると共に定期的に見直しを行って、特権的なユーティリティプログラムが適切に実行されるように管理しています。

5.3.5 仮想コンピューティング環境における分離

<ISO/IEC 27017 CLD.9.5.1>

FJcloud-O / FJcloud-ベアメタルでは、システムを構成するサーバ、ストレージ、ネットワーク等の機器を大規模に用意し、適切に管理しています。また、障害や事故、災害時に備えて迅速に事業継続ができるように必要な予備・冗長化構成を整備しています。

これらの機器に対して、お客様が利用する機器とサービス基盤のための機器を物理的に分離して構成しています。また、仮想化技術やネットワークセキュリティ技術を適用し、各サービス利用者に対して、仮想サーバ、仮想ストレージ、仮想ネットワー

クといったリソースをオンデマンドで提供しています。これらの仮想リソースはお客様ごとに論理的または物理的（ベアメタルサービスの場合）に分離して管理しています。

FJcloud-O における PaaS サービスでは、各 PaaS サービスの特性に応じて、利用者ごとに環境を分離しています。詳しくは各 PaaS サービスのサービス仕様書を参照してください。

5.3.6 仮想マシンの要塞化

<ISO/IEC 27017 CLD.9.5.2>

FJcloud-O / FJcloud-ベアメタルにおけるお客様の仮想マシンのセキュリティ対策については、お客様の責任で実施していただく必要があります。仮想マシン配備時の初期設定内容、お客様が実施するセキュリティ対策のための仮想ルータ、ファイアウォール、セキュリティグループ及びそれらのログ取得などについては、「FUJITSU Hybrid IT Service FJcloud-O IaaS 機能説明書」等を参照してください。

また、FJcloud-O の各 PaaS におけるお客様環境でのセキュリティ対策については、各 PaaS サービスの特性に応じて対策内容が異なりますので、利用される PaaS のサービス仕様書を参照してください。

5.3.7 暗号による管理策の利用方針

<ISO/IEC 27017 10.1.1>

FJcloud-O サービス / FJcloud-ベアメタルサービスを利用するお客様の環境で扱うお客様の情報資産については、お客様の責任で管理策を実施していただきます。なお、お客様がポータルや API へアクセスする場合のインターネット通信は FJcloud-O / FJcloud-ベアメタルが暗号化しています。

FJcloud-O / FJcloud-ベアメタルのサービス基盤運用で取り扱う情報資産については、当社のセキュリティ管理規程及び実施基準などの規程に基づいて、情報資産の重要度に応じてストレージや通信の暗号化を適切に実施しています。 各サービス基盤の運用においても、SSL-VPN を用いたセキュアな通信方式を採用しています。

5.3.8 鍵管理

<ISO/IEC 27017 10.1.2>

FJcloud-O / FJcloud-ベアメタルのサービス基盤運用では、破壊、改竄されないように、さらに情報漏えいしないように適切に鍵管理のポリシーや手順を定めて、対策を実施しています。また、万が一鍵の事故、または危殆化が発生した場合についても対策しています。

5.4 通信のセキュリティ

5.4.1 ネットワークの分離

<ISO/IEC 27017 13.1.3>

FJcloud-O サービス / FJcloud-ベアメタルサービスでは、お客様が利用するリソースとサービス管理のための領域を、ネットワークを含めて分離しています。また、お客様の仮想リソースもネットワークを含めて、分離する機能を提供しています。

5.4.2 仮想及び物理ネットワークのセキュリティ管理の整合

<ISO/IEC 27017 CLD.13.1.4>

FJcloud-O / FJcloud-ベアメタルのサービス基盤を管理するネットワークは、お客様が利用する仮想リソースにアクセスするネットワークと物理的に分離しています。また、必要な通信のみを許可し、ウィルス対策や不正アクセス検知装置（IDS）、ファイアウォールなどの技術的な対策を実施しています。さらに、定期的なルータやファイアウォールルールなどのネットワーク設定のレビューや外部・内部のぜい弱性スキャンや社内の有資格者によるペネトレーションテストなどを実施して、物理と仮想のネットワークの整合性及びセキュアな通信を保っています。

5.5 運用管理

5.5.1 変更管理

<ISO/IEC 27017 12.1.2, CLD.12.1.5>

FJcloud-O / FJcloud-ベアメタルでは、システムコンポーネントに関する全ての変更において、変更管理及びリリース管理プロセスを定め、それに則って変更・リリース作業を実施しています。定型の変更業務については、作業の異常発生時のバックアウト手順を含めた作業手順書を整備し、試験した後に管理者が変更の承認を実施しています。また、システムを変更した後の稼働チェック合否判定基準を設け、システム品質が基準を満たしていることを確認するための体系的なモニタリングと評価プログラムを整備しています。変更作業においては、オペレーションの監視やチェックなど複数名でチェックを実施しています。また、併せてプログラムによる自動化を含めた品質確保も実施しています。

なお、FJcloud-O / FJcloud-ベアメタルでは、お客様業務に影響があるシステム変更やリリースは、利用規約に定める予告期間を持って、変更後の内容をお客様に通知します。（緊急メンテナンス作業は、この限りではありません。）

5.5.2 容量・能力の管理

<ISO/IEC 27017 12.1.3>

お客様がオンデマンドで仮想リソースを作成・利用できるように、FJcloud-O / FJcloud-ベアメタルではコンピューティング資源の枯渇を未然に防ぐためのキャパシティ管理プロセスを定め、それに則って適切な管理を継続的に実施しています。具体的には、監視対象、監視内容、監視方法を決めて監視を行うと共に、過去の利用状況・実績値などを基にした利用予測を行い、適時コンピューティング資源を増強しています。

5.5.3 情報のバックアップ

<ISO/IEC 27017 12.3.1>

FJcloud-O / FJcloud-ベアメタルでは、障害や事故、災害時に備えて迅速に事業継続ができるように、サービス管理のための情報資産等の定期バックアップを取得しています。

5.5.4 イベントログ取得

<ISO/IEC 27017 12.4.1>

FJcloud-O サービス / FJcloud-ベアメタルサービスにおけるお客様の利用環境については、お客様の責任で各種ログを取得してください。

また、ポータル及び API へのアクセスログについては、各サービスでログを取得し、一定期間保管すると共に、定期的なチェックによる監視をしています。

5.5.5 実務管理者及び運用担当者の作業ログ

<ISO/IEC 27017 12.4.3>

FJcloud-O サービス / FJcloud-ベアメタルサービスに係わる要員の情報システムにアクセスした各種ログや運用専用ルームへの入退室ログを取得し、定期的にレビューを実施しています。また、一定期間保存し、不正防止やインシデント発生を予防しています。

5.5.6 クロックの同期

<ISO/IEC 27017 12.4.4>

FJcloud-O / FJcloud-ベアメタルのサービス基盤は、NTP(Network Time Protocol)を用いて複数サービスの時刻をUTC（Coordinated Universal Time）基準とした時刻に同期しています。具体的には、サービス提供しているリージョンごとに同期する上位 NTP サーバを信頼できる複数の公開サーバから選定し、取得して実現しています。
お客様の利用する仮想リソースの時刻同期については、「FUJITSU Hybrid IT Service FJcloud-O IaaS 機能説明書」を参照してください。

5.5.7 クラウドサービスの監視

<ISO/IEC 27017 CLD.12.4.5>

FJcloud-O / FJcloud-ベアメタルでは、サービスを構成する各機器、システムの性能・リソース・API などについて監視を実施しています。さらに、異常を迅速に検知・通知する監視を実施しています。また、サービス全体の監視のため、サービスを提供するリージョン間で死活監視を相互に行う仕組みを導入してサービスの継続性を維持しています。また、異常を検知した場合に自動リカバリを実施する仕組みについても、順次強化する取組みを行っています。

お客様の利用環境における仮想リソースやお客様環境で実行するアプリケーションの監視については、お客様の責任で実施していただきます。なお、お客様の利用する仮想リソースやその上で動作するアプリケーションのモニタリング用に FJcloud-O / FJcloud-ベアメタルが監視サービスを提供しています。

5.5.8 技術的ぜい弱性の管理

<ISO/IEC 27017 12.6.1>

FJcloud-O / FJcloud-ベアメタルでは、ポータルなどを始めとするサービス管理を行うための Web アプリケーションについては、社内の制度に基づいて、ぜい弱性を悪用した不正アクセスからシステムを守るため、サービス機能のリリース前にぜい弱性診断ソフトウェアを使用した情報セキュリティ検査を実施しています。また、ウィルス感染から保護するアンチウィルスソフトウェアは定期的にシグネチャを更新しています。

FJcloud-O サービス / FJcloud-ベアメタルサービスを提供するための基盤については、セキュリティの脅威（不正アクセス、不正プログラムなど）やぜい弱性に対して迅速に対応できるよう組織内セキュリリティ専門チームである SOC を設け、脅威やぜい弱性に関する情報を FIRST[2]、JPCERT/CC[3]、日本 CSIRT 協議会[4]などの外部機関からの提供や独自収集により入手し、それらのリスクをコントロールしています。ぜい弱性パッチの管理についてポリシーと手順を定めて、ベンダから提供されたセキュリティパッチの優先度付けと影響評価を行っています。さらにぜい弱性診断を定期的に行っています。

なお、富士通では、「Open Web Application Security Project Guide」などの安全なコーディングを行うためのガイドラインを参考に Web アプリケーションを開発しています。併せて、クロスサイトスクリプティング対策やインジェクション対策の不備など Web アプリケーションのぜい弱性に対応するための監査制度に則った情報セキュリティ検査を Web アプリケーションの開発プロセスに組み込んでいます。

5.6 セキュリティインシデント

5.6.1 情報セキュリティインシデント管理

<ISO/IEC 27017 16.1.1>

<ISO/IEC 27017 16.1.2>

FJcloud-O / FJcloud-ベアメタルでは、情報セキュリティインシデントは、お客様からの問い合わせやサービス基盤のトラブルなどのインシデントと共通の管理ポリシー、プロセス、および手順を定めています。情報セキュリティインシデントが発生した際にも、これに従って情報セキュリティに関するイベントの識別と報告を迅速かつ確実に行っています。お客様が利用しているリソース

---

[2] 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。67 を超える国と地域の CSIRT がメンバーとして登録され、その数は 400 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。

[3] 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。

[4] 日本 CSIRT 協議会（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。

に影響がある可能性のあるインシデントやデータ侵害の可能性のあるインシデントの発生時には、メール等の手段により通知を行っています。

なお、通知は FJcloud-O / FJcloud-ベアメタルにおけるサービス障害のほか、お客様が禁止事項に抵触した際の FJcloud-O / FJcloud-ベアメタル側での対応結果やお客様の利用環境内で問題が発生している可能性のある事象を検知した確認依頼も含まれます。

お客様が利用しているリソースにおいて、FJcloud-O / FJcloud-ベアメタルの SLA 判定基準に該当する障害発生を富士通が確認した場合、その通知については 1 時間以内を目標としています。

FJcloud-O / FJcloud-ベアメタルでは、過去の障害情報を蓄積・分析することにより、トラブルの再発防止に継続的に取り組んでいます。

5.6.2 証拠の収集

<ISO/IEC 27017 16.1.7>

FJcloud-O / FJcloud-ベアメタルでは、お客様が情報セキュリティインシデントの解決のために必要となるサービス基盤内のログなどのデジタル証拠について開示が必要な場合、ヘルプデスクにお問い合わせやご相談をお願いいたします。

なお、富士通では FJcloud-O / FJcloud-ベアメタルのサービス提供基盤のセキュリティ問題のご報告を受け付ける窓口を設置しています。ご報告いただいた内容は、CERT 部門を中心に社内関係組織および外部の専門組織・所轄官庁と連携し、適切に対処・報告します。

5.6.3 情報セキュリティ継続の計画

<ISO/IEC 27001 17.1.1>

大規模災害等の不測の事態発生時にも、重要な事業を継続するためには、自社を取り巻くリスク環境や経営環境に合わせた事業継続管理が重要です。富士通は、事業継続管理のために、経営者の積極的な関与のもと、事業継続計画の策定と対策の実施、計画の継続的な改善活動に取り組んでいます。

FJcloud-O / FJcloud-ベアメタルでは、ストレージ、サーバ、ネットワークなどサービス基盤を構成する機器や電源設備、および機器を接続するケーブルのルートなどを含む主要コンポーネントは、障害や事故、災害時に備えて、安定して事業継続ができるように必要な予備、冗長構成を整備し、単一故障点を排除しています。ストレージ機器については、RAID6 相当の冗長化を行っています。また、ハード障害が発生した場合、自動的にフェールオーバーし事業継続性を確保します。

FJcloud-O / FJcloud-ベアメタルでは、サービスを提供するリージョンでは、電源系統などの DC ファシリティが異なるアベイラビリティーゾーンを提供し、複数のアベイラビリティーゾーンにお客様システムを展開することで、お客様の業務が継続できるようにしています。詳しくは「FUJITSU Hybrid IT Service FJcloud-O IaaS サービス仕様書」等を参照ください。また、サービスレベルについては「FUJITSU Hybrid IT Service FJcloud サービスレベル仕様書」を参照ください。

5.7 システム開発及び保守

5.7.1 情報セキュリティ要求事項の分析及び仕様化

<ISO/IEC 27017 14.1.1>

FJcloud-O / FJcloud-ベアメタルでは、情報セキュリティ実施基準として、各サービスのセキュリティを維持するためのセキュリティ管理の方針、及び実施や運用などサービスのライフサイクル全般に渡り、考慮すべき要件を定め、これに従って適切にサービスを運営しています。

サービス基盤に導入する製品やサービスについて、機能、性能、サポートなどに関する採用基準を定め、それに基づく評価をした上で導入する体制を構築しています。他システムとの整合性など結合テストを含めて確認しています。

5.7.2 セキュリティに配慮した開発のための方針

<ISO/IEC 27017 14.2.1>

提供するサービスの環境や機能などの相違を考慮し、IaaS 及び PaaS それぞれの開発実施基準を定め、これに従ったサービス開発を実施しています。これらは「セキュリティ・バイ・デザイン」の考え方に基づいており、設計段階からセキュリティ要件を考慮した開発を実施すると共に、社内の各種ガイドラインや社内の監査制度に従ったプログラム開発に取り組んでおり、これらの基準や監査に合格したもののみサービス提供をしています。また、開発環境と本番環境の完全な分離、ぜい弱性スキャンの実施など、開発における各プロセスで適切にセキュリティを確保した開発を実施しています。

6　供給者との関係

6.1 供給者関係のための情報セキュリティの方針

<ISO/IEC 27017 15.1.1>

<ISO/IEC 27017 15.1.2>

委託先の決定にあたっては、責任者の承認を得て行うのはもちろん、安全確保のため、機密保護、安全な運行等に関する項目を盛り込んだ契約を締結しています。

6.2 ICT サプライチェーン

<ISO/IEC 27017 15.1.3>

FJcloud-O / FJcloud-ベアメタルを構成するデータセンターや機器の供給については、富士通のセキュリティ方針に沿うようにリスク管理をしています。

他社からサービスを受ける場合には、供給者に対して情報セキュリティ方針と適合する情報セキュリティ目的を示し、それを達成するためのリスクマネジメント活動の実施を要求しています。

7　順守

7.1 適用法令及び契約上の要求事項の特定

<ISO/IEC 27017 18.1.1>

FJcloud-O / FJcloud-ベアメタルは、お客様からお預かりした大切な情報を法令に沿って適切に取扱い、お客様の権利および利益を保護しています。その上で、以下の項目等を「FUJITSU Hybrid IT Service FJcloud 利用規約」等で明示しています。

- お客様がクラウドサービスに登録および入力したお客様固有の情報などに関する秘密情報の取扱い
- お客様が契約に違反していると判断した場合に、富士通が該当する情報の送信を遮断すること、および表示する情報を削除または不表示とすること
- 準拠法や管轄裁判所に関する情報（リージョン特約条項で合意した内容が適用されます[5]）

なお、捜査当局や裁判所等の機関からの開示要求については、富士通において定められたプロセス・手順により判断を行っております。

7.2 知的財産権

<ISO/IEC 27017 18.1.2>

知的財産権及び権利関係のあるソフトウェア製品の利用に関連する取扱については、利用規約に示してあります。

7.3 記録の保護

<ISO/IEC 27017 18.1.3>

[5] 日本リージョンにおいて、「FUJITSU Hybrid IT Service FJcloud 日本リージョンでの契約にかかるリージョン特約条項」での合意した場合、準拠法は日本法、契約に関する訴訟については、東京地方裁判所が第一審の専属的合意管轄裁判所となります。

クラウドサービスを利用する上で、さまざまな法令や規制の要求に沿ってコンプライアンスを維持していくことは、お客様にとって重要な課題です。コンプライアンスの順守状況を監査するために、クラウドサービスの利用者のアクセスや操作などを後から調査できるようにログが適切に記録されていなければなりません。

FJcloud-O / FJcloud-ベアメタルでは、お客様がコンプライアンスの維持と監査に対応するため、サービス運用者が行った作業のログを証跡として記録し、一定期間保存しています。

また、GDPR[6]に準拠するため、FJcloud-O / FJcloud-ベアメタルは処理者として、管理者または処理者に代わって行った顧客データの取扱記録についても、一定期間保管します。

7.4 暗号化機能に対する規制

<ISO/IEC 27017 18.1.5>

FJcloud-O / FJcloud-ベアメタルでは、お客様がインターネット経由でポータルや API にアクセスする際、経路を SSL/TLS プロトコルにより暗号化しています。暗号化に利用するアルゴリズムは、日本国政府（総務省及び経済産業省）が策定する「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト)」を参考としており、輸出規制の対象となるものは使用していません。

7.5 情報セキュリティの独立したレビュー

<ISO/IEC 27017 18.2.1>

年一回もしくは大きな組織変更やシステムの大幅な改版があった場合に、情報セキュリティの方針群をレビューし必要に応じてビジネス目標やリスク環境の変化を反映して見直しています。また、情報セキュリティ要求事項のベースラインおよびガイドラインを基にアプリケーションやデータベース、システム及びネットワークインフラストラクチャの設計と実装に適用しています。これらの基準への適合状況の確認のため、内部監査を定期的（=年一回以上）に実施することを定め、FJcloud-O / FJcloud-ベアメタルおよびその運営組織に対して監査を実施し、予防や是正に取り組んでいます。

FJcloud-O / FJcloud-ベアメタルが取得または受領している第三者による認証および保証報告書は以下のものがあります。

- ISO/IEC27001:2013/JIS Q 27001:2014
- JIP-ISMS517-1.0(ISO/IEC27017:2015)
- PCI DSS 準拠証明書（AOC）
- SOC2（および FISC 安全対策基準）Type2 保証報告書

FJcloud-O / FJcloud-ベアメタルは、複数のお客様に同時に利用頂くサービスのため、運用拠点やデータセンターなどの直接的な監査要求は受け入れておりません。監査に関する情報提供が必要な場合は、富士通の窓口に個別にご相談下さい。

8 おわりに

富士通では、本書で説明した情報セキュリティの基本方針に基づき、情報セキュリティ対策を継続的に実施、改善、向上していきます。また、継続的にクラウドに対する様々な脅威に対応していきます。

お客様の事業やサービスを創造するための基盤として、FUJITSU Hybrid IT Service FJcloud-O / FJcloud-ベアメタル を安心してご活用下さい。

---

[6] GDPR(General Data Protection Regulation) : EU データ一般保護規則。EU 加盟国における統一的な個人データの保護に関する法律（日本の個人情報保護法に相当）です。

Appendix A：用語集

表 A-1 用語集(1/1)

用　語	内　容
API	あるプラットフォーム（OS やミドルウェア）向けのソフトウェアを開発する際に使用できる命令や関数の集合のこと。
FeliCa カード	非接触型 IC カードのための通信技術として開発されたカード。
FISC 安全対策基準	公益財団法人　金融情報システムセンター(The Center for Financial Industry Information Systems：以下、FISC)が定める安全対策基準
FUJITSU Way	富士通グループの理念・指針のこと。富士通グループが経営革新とグローバルな事業展開を推進していく上で不可欠なグループ全体の求心力の基となる企業理念、価値観及び社員一人ひとりがどのように行動すべきかの原理原則を示したもの。 http://jp.fujitsu.com/about/corporate/philosophy/
GDPR	General Data Protection Regulation の略称で、日本では「EU 一般データ保護規則」といい、EU 加盟国における統一的な個人データの保護に関する法律である。主に、EEA (*)在住者の個人データの「処理」と「移転」に関するルールを規定している。 (*)EEA(European Economic Area)：EU 加盟 28 か国+3 か国(アイスランド、リヒテンシュタイン、ノルウェー)の 31 か国。当該国に在住する個人の個人データが対象。
IaaS	Infrastructure as a Service の略称。サーバ、ストレージ、OS、ミドルウェアなどのシステムリソースをサービスとして利用できる IT の利用形態。
IDS(不正アクセス検知装置)	Intrusion Detection System の略称で、不正アクセス検知機能をもつ装置をいう。
ISO/IEC27001:2013/JIS Q27001:2014	Certificate of Registration -ISO/IEC27001:2013/JIS Q27001:2014 情報セキュリティマネジメントシステム（ISMS） 情報技術–セキュリティ技術–情報セキュリティマネジメントシステム–要求事項
JIP-ISMS517-1.0(ISO/IEC27017:2015)	Certificate of Registration -ISO/IEC27017:2015/JIP-ISMS517-1.0 ISMS クラウドセキュリティ 情報技術-セキュリティ技術-ISO/IEC27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範
PaaS	Platform as a Service の略称。アプリケーション開発・実行・運用環境、ユーティリティをサービスとして利用できる IT の利用形態。
PCI DSS 準拠証明書（AOC）	Payment Card Industry Data Security Standard の略称。国際カードブランド 5 社が策定したクレジットカード情報取引情報の安全な管理を評価するためのグローバルセキュリティ基準のこと。 https://ja.pcisecuritystandards.org/minisite/en/pci-dss.php
SOC2（および FISC 安全対策基準）Type2 保証報告書	FUJITSU Hybrid IT Service FJcloud-O のシステムに係る「セキュリティ」および「可用性」の記述書ならびに内部統制のデザインの適切性に係る報告書 米国公認会計士協会（AICPA）とカナダ勅許会計士会（CICA）が制定した Trust サービス原則（Trust Services Principles and Criteria）。この原則に基づいて、外部監査機関がサービス提供組織の内部統制について客観的に検証し、該当基準を満たしていると認めた場合にのみ発行するのが、SOC2 保証報告書。
SSL/TLS プロトコル	SSL（Secure Sockets Layer）/TLS（Transport Layer Security）は、インターネット上でデータを暗号化して送受信できるトランスポート層のプロトコル。
SSL-VPN	Secure Sockets Layer virtual private network の略称で、暗号通信に SSL を使用し、VPN によって、イントラネットなどのプライベートネットワークが、本来公的なネットワークであるインターネットに跨って、まるで各プライベートネットワーク間が専用線で接続されているかのように実現される技術。
ベアメタルサービス	クラウド上で専有物理サーバを提供するサービス。

Appendix B：ISO/IEC27001、ISO/IEC27017 の管理策と本書目次との対応関係について

表 B-1 ISO/IEC27001、ISO/IEC27017 の管理策と本書目次との対応表(1/3)

ISO/IEC 27001 管理策番号	管理策	本書の該当目次
A.5.1.1	情報セキュリティのための方針群	2.
A.5.1.2	情報セキュリティのための方針群のレビュー	
A.6.1.1	情報セキュリティの役割及び責任	3.1
A.6.1.2	職務の分離	
A.6.1.3	関係当局との連絡	3.1
A.6.1.4	専門組織との連絡	
A.6.1.5	プロジェクトマネジメントにおける情報セキュリティ	
A.6.2.1	モバイル機器の方針	
A.6.2.2	テレワーキング	
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	3.2
A.7.1.1	選考	
A.7.1.2	雇用条件	
A.7.2.1	経営陣の責任	
A.7.2.2	情報セキュリティの意識向上、教育及び訓練	4.1
A.7.2.3	懲戒手続	
A.7.3.1	雇用の終了又は変更に関する責任	
A.8.1.1	資産目録	4.2
A.8.1.2	資産の管理責任	
A.8.1.3	資産利用の許容範囲	
A.8.1.4	資産の返却	
CLD.8.1.5	クラウドサービスカスタマの資産の除去	4.3
A.8.2.1	情報の分類	
A.8.2.2	情報のラベル付け	4.2
A.8.2.3	資産の取扱い	
A.8.3.1	取外し可能な媒体の管理	
A.8.3.2	媒体の処分	
A.8.3.3	物理的媒体の輸送	
A.9.1.1	アクセス制御方針	5.2.1 5.3.1
A.9.1.2	ネットワーク及びネットワークサービスへのアクセス	5.3.2
A.9.2.1	利用者登録及び登録削除	5.3.3
A.9.2.2	利用者アクセスの提供（provisioning）	5.3.3
A.9.2.3	特権的アクセス権の管理	5.3.4
A.9.2.4	利用者の秘密認証情報の管理	5.3.3
A.9.2.5	利用者アクセス権のレビュー	
A.9.2.6	アクセス権の削除又は修正	
A.9.3.1	秘密認証情報の利用	
A.9.4.1	情報へのアクセス制限	5.3.4
A.9.4.2	セキュリティに配慮したログオン手順	
A.9.4.3	パスワード管理システム	5.3.4
A.9.4.4	特権的なユーティリティプログラムの使用	5.3.4
A.9.4.5	プログラムソースコードへのアクセス制御	
CLD.9.5.1	仮想コンピューティング環境における分離	5.3.5
CLD.9.5.2	仮想マシンの要塞化	5.3.6
A.10.1.1	暗号による管理策の利用方針	5.3.7
A.10.1.2	鍵管理	5.3.8

表 B-2 ISO/IEC27001、ISO/IEC27017 の管理策と本書目次との対応表(2/3)

ISO/IEC 27001 管理策番号	管理策	本書の該当目次
A.11.1.1	物理的セキュリティ境界	
A.11.1.2	物理的入退管理策	
A.11.1.3	オフィス，部屋及び施設のセキュリティ	
A.11.1.4	外部及び環境の脅威からの保護	
A.11.1.5	セキュリティを保つべき領域での作業	
A.11.1.6	受渡場所	
A.11.2.1	装置の設置及び保護	
A.11.2.2	サポートユーティリティ	
A.11.2.3	ケーブル配線のセキュリティ	
A.11.2.4	装置の保守	
A.11.2.5	資産の移動	
A.11.2.6	構外にある装置及び資産のセキュリティ	
A.11.2.7	装置のセキュリティを保った処分又は再利用	5.2.2
A.11.2.8	無人状態にある利用者装置	
A.11.2.9	クリアデスク・クリアスクリーン方針	
A.12.1.1	操作手順書	
A.12.1.2	変更管理	5.5.1
A.12.1.3	容量・能力の管理	5.5.2
A.12.1.4	開発環境，試験環境及び運用環境の分離	
CLD.12.1.5	実務管理者の運用のセキュリティ	5.5.1
A.12.2.1	マルウェアに対する管理策	
A.12.3.1	情報のバックアップ	5.5.3
A.12.4.1	イベントログ取得	5.5.4
A.12.4.2	ログ情報の保護	
A.12.4.3	実務管理者及び運用担当者の作業ログ	5.5.5
A.12.4.4	クロックの同期	5.5.6
CLD.12.4.5	クラウドサービスの監視	5.5.7
A.12.5.1	運用システムに関わるソフトウェアの導入	
A.12.6.1	技術的ぜい弱性の管理	5.5.8
A.12.6.2	ソフトウェアのインストールの制限	
A.12.7.1	情報システムの監査に対する管理策	
A.13.1.1	ネットワーク管理策	
A.13.1.2	ネットワークサービスのセキュリティ	
A.13.1.3	ネットワークの分離	5.4.1
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	5.4.2
A.13.2.1	情報転送の方針及び手順	
A.13.2.2	情報転送に関する合意	
A.13.2.3	電子的メッセージ通信	
A.13.2.4	秘密保持契約又は守秘義務契約	
A.14.1.1	情報セキュリティ要求事項の分析及び仕様化	5.7.1
A.14.1.2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮	
A.14.1.3	アプリケーションサービスのトランザクションの保護	
A.14.2.1	セキュリティに配慮した開発のための方針	5.7.2
A.14.2.2	システムの変更管理手順	
A.14.2.3	オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー	
A.14.2.4	パッケージソフトウェアの変更に対する制限	

表 B-3 ISO/IEC27001、ISO/IEC27017 の管理策と本書目次との対応表(3/3)

ISO/IEC 27001 管理策番号	管理策	本書の該当目次
A.14.2.5	セキュリティに配慮したシステム構築の原則	
A.14.2.6	セキュリティに配慮した開発環境	
A.14.2.7	外部委託による開発	
A.14.2.8	システムセキュリティの試験	
A.14.2.9	システムの受入れ試験	
A.14.3.1	試験データの保護	
A.15.1.1	供給者関係のための情報セキュリティの方針	6.1
A.15.1.2	供給者との合意におけるセキュリティの取扱い	6.1
A.15.1.3	ICT サプライチェーン	6.2
A.15.2.1	供給者のサービス提供の監視及びレビュー	
A.15.2.2	供給者のサービス提供の変更に対する管理	
A.16.1.1	責任及び手順	5.6.1
A.16.1.2	情報セキュリティ事象の報告	5.6.1
A.16.1.3	情報セキュリティ弱点の報告	
A.16.1.4	情報セキュリティ事象の評価及び決定	
A.16.1.5	情報セキュリティインシデントへの対応	
A.16.1.6	情報セキュリティインシデントからの学習	
A.16.1.7	証拠の収集	5.6.2
A.17.1.1	情報セキュリティ継続の計画	5.6.3
A.17.1.2	情報セキュリティ継続の実施	
A.17.1.3	情報セキュリティ継続の検証，レビュー及び評価	
A.17.2.1	情報処理施設の可用性	
A.18.1.1	適用法令及び契約上の要求事項の特定	7.1
A.18.1.2	知的財産権	7.2
A.18.1.3	記録の保護	7.3
A.18.1.4	プライバシー及び個人を特定できる情報（PII）の保護	
A.18.1.5	暗号化機能に対する規制	7.4
A.18.2.1	情報セキュリティの独立したレビュー	7.5
A.18.2.2	情報セキュリティのための方針群及び標準の順守	
A.18.2.3	技術的順守のレビュー	