金融機関向け
『IBM Cloud』対応セキュリティリファレンス

2020年02月28日

Version 1.0.0

作成者:
株式会社三菱総合研究所(MRI)

更新日	版番号	改版内容
2020年2月28日	Version1.0.0	初版

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
統1	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における規程は、利用者が整備を行う必要がある。クラウド事業者に関連する規程に関しては、「2 外部の統制」の内容を踏まえ決定を行うことが望ましい。
統2	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における計画は、利用者が策定を行う必要がある。クラウド事業者の新機能提供予定を考慮する場合は、公開資料の参照を行うか、必要に応じてヒアリング等を行うことが考えられる。
統3	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における計画は、利用者が策定を行う必要がある。クラウド事業者の新機能提供予定を考慮する場合は、公開資料の参照を行うか、必要に応じてヒアリング等を行うことが考えられる。
統4	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における体制は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統5	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における態勢は、利用者が整備する必要がある。クラウド事業者への態勢確認、対応手順の確認は「2 外部の統制」の内容を踏まえて実施することが望ましい。
統6	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における体制は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統7	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における体制は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統8	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における体制は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統9	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における組織は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統10	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における組織は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統11	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における組織は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統12	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における組織は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統13	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における組織は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統14	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における教育は、利用者が実施する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統15	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における教育は、利用者が実施する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統16	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における教育は、利用者が実施する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統17	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における訓練は、利用者が実施する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統18	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における管理は、利用者が実施する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統19	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者における管理は、利用者が実施する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
統20	・日本国内のデータセンタを貸借するにあたり、全世界のデータセンタと同様に機密保護および安全運行に関する委託契約を締結済みです。 ・外部委託を行う場合、利用企業は外部委託管理の義務が生じます。各データセンターおよびサーバールームの運用管理状況は、外部監査などの第三者機関による監査により、その妥当性および透明性が確保されます。 ・IBM Cloud の各データセンターの運用状況は、委託しているデータセンター事業者による監視が行われる他、各データセンターには常勤の IBM 従業員の設備責任者が配置され、データセンターの安全管理を監視し、改善が必要となる場合には速やかに連携する体制がとられます。 ・IBM Cloudに関する管理運用は、IBMグループ社員によって運用されており、他社への再委託はありません。 ・利用者内部は、利用者にて整備を行っていただく前提となっています。 <ご参考> ・IBM Cloud セキュリティガイドブック ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・SoftLayer Technologies, Inc. Infrastructure as a Service (IaaS) System 3 SOC 3 Report Relevant to the Security and Availability Principles ・ SOFTLAYER_US_SoftLayer SOC 1 2H 2017 Report ・A guide to IBM Bluemix resiliency and security	適合可能	文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 15.1.1 供給者関係のための情報セキュリティの方針 JIS Q 27002 の15.1.1 に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。 NDA文献[N02]にて、外部委託選定の際の承認ルールと、セキュリティルールを定めていることを確認した。 文献[01]の「3.3. 外部委託管理」にて、サーバー（コンピューター資源）やネットワークに関する管理運用はIBM社員によって運用されており、他社への再委託はないことを確認した。 文献[01]の「3.3. 外部委託管理」にて、データセンターはデータセンター事業者への委託となっているため、データセンター自体の管理運用、入退室管理等については委託先であるデータセンター事業者に託しているが、外部監査などの第三者機関による監査により、管理状況は全て透明性を以って開示しており、日本の上場企業の要求に十分に耐えうるサービスを提供していることを確認した。	要NDA	文献[01] 文献[09]	ISO27017 15.1.1	―	NDA文献[N02]	利用者は選定手続きを明確にし、客観的評価をもとに委託可否を決定し、責任者の承認を得る必要がある。
統21	・日本国内のデータセンタを貸借するにあたり、全世界のデータセンタと同様に機密保護および安全運行に関する委託契約を締結済みです。 ・外部委託を行う場合、利用企業は外部委託管理の義務が生じます。各データセンターおよびサーバールームの運用管理状況は、外部監査などの第三者機関による監査により、その妥当性および透明性が確保されます。 ・IBM Cloud の各データセンターの運用状況は、委託しているデータセンター事業者による監視が行われる他、各データセンターには常勤の IBM 従業員の設備責任者が配置され、データセンターの安全管理を監視し、改善が必要となる場合には速やかに連携する体制がとられます。 ・IBM Cloudに関する管理運用は、IBMグループ社員によって運用されており、他社への再委託はありません。 ・利用者内部は、利用者にて整備を行っていただく前提です。 <ご参考> ・IBM Cloud セキュリティガイドブック ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・SoftLayer Technologies, Inc. Infrastructure as a Service (IaaS) System 3 SOC 3 Report Relevant to the Security and Availability Principles ・ SOFTLAYER_US_SoftLayer SOC 1 2H 2017 Report ・A guide to IBM Bluemix resiliency and security ″	適合可能	文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 15.1.3 ICT サプライチェーン JIS Q 27002 の15.1.3 に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。 NDA文献[N02]にて、外部委託選定の際の承認ルールと、セキュリティルールを定めていることを確認した。 文献[01]の「3.3. 外部委託管理」にて、サーバー（コンピューター資源）やネットワークに関する管理運用はIBM社員によって運用されており、他社への再委託はないことを確認した。 文献[01]の「3.3. 外部委託管理」にて、データセンターはデータセンター事業者への委託となっているため、データセンター自体の管理運用、入退室管理等については委託先であるデータセンター事業者に託しているが、外部監査などの第三者機関による監査により、管理状況は全て透明性を以って開示しており、日本の上場企業の要求に十分に耐えうるサービスを提供していることを確認した。	要NDA	文献[01] 文献[09]	ISO27017 15.1.3	―	NDA文献[N02]	利用者は契約時に考慮すべき事項を盛り込み、契約締結手続きを行う必要がある。 また、サービス条件等について定期的に確認を行う必要がある。
統22	・外部委託を行う場合、利用企業は外部委託管理の義務が生じます。IBM Cloud では、データセンターはTier3以上のレベルの外部のデータセンター事業者へ委託します。各データセンターおよびサーバールームの運用管理状況は、外部監査などの第三者機関による監査により、その妥当性および透明性が確保されます。 ・IBM Cloud の各データセンターの運用状況は、委託しているデータセンター事業者による監視が行われる他、各データセンターには常勤の IBM 従業員の設備責任者が配置され、データセンターの安全管理を監視し、改善が必要となる場合には速やかに連携する体制がとられます。 ・IBM Cloudに関する管理運用は、IBMグループ社員によって運用されており、他社への再委託はありません。 ・利用者内部は、利用者にて整備を行っていただく前提です。 <ご参考> ・IBM Cloud セキュリティカ ゛イト ゛フ ゛ック ・技術よりな人か ゛最初に読む:IBMCloud柔らか層本 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・SoftLayer Technologies, Inc. Infrastructure as a Service (IaaS) System 3 SOC 3 Report Relevant to the Security and Availability Principles ・ SOFTLAYER_US_SoftLayer SOC 1 2H 2017 Report ・A guide to IBM Bluemix resiliency and security	適合可能	文献[01]の「3.3. 外部委託管理」にて、データセンターはデータセンター事業者への委託となっておりますので、データセンター自体の管理運用、入退室管理 等については委託先であるデータセンター事業者に託しておりますが、外部監査などの第三者機関による監査により、管理状況は全て透明性を以って開示しており、日本の上場企業の要求に十分に耐えうるサービスを提供していることを確認した。	公開文書	文献[01]	―	―	―	利用者は、委託業務におけるセキュリティポリシー等のルールの遵守状況を定期的に確認する必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
統23	・外部委託を行う場合、利用企業は外部委託管理の義務が生じます。IBM Cloud では、データセンターはTier3以上のレベルの外部のデータセンター事業者へ委託します。各データセンターおよびサーバールームの運用管理状況は、外部監査などの第三者機関による監査により、その妥当性および透明性が確保されます。 ・IBM Cloud の各データセンターの運用状況は、委託しているデータセンター事業者による監視が行われる他、各データセンターには常勤の IBM 従業員の設備責任者が配置され、データセンターの安全管理を監視し、改善が必要となる場合には速やかに連携する体制がとられます。 ・IBM Cloudに関する管理運用は、IBMグループ社員によって運用されており、他社への再委託はありません。 ・利用者内部は、利用者にて整備を行っていただく前提です。 〈ご参考〉 ・IBM Cloud セキュリティカ゛イト゛フ゛ック ・技術よりな人か゛最初に読む:IBMCloud柔らか層本 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・SoftLayer Technologies, Inc. Infrastructure as a Service (IaaS) System 3 SOC 3 Report Relevant to the Security and Availability Principles ・ SOFTLAYER_US_SoftLayer SOC 1 2H 2017 Report ・A guide to IBM Bluemix resiliency and security	適合可能	文献[03]の239スライド目にて、データセンターセキュリティについては、第三者による監査業者が継続的に監査を実施（SOC2などの外部監査業者による認証取得）していることを確認した。 文献[01]の「3.3. 外部委託管理」にて、データセンターはデータセンター事業者への委託となっているため、データセンター自体の管理運用、入退室管理等については委託先であるデータセンター事業者に託しているが、外部監査などの第三者機関による監査により、管理状況は全て透明性を以って開示しており、日本の上場企業の要求に十分に耐えうるサービスを提供していることを確認した。	公開文書	文献[01] 文献[03]	–	–	–	利用者は委託業務の遂行状況を定期的に確認する必要がある。
統24	内容確認中 ・直接の内部統制が及びにくいというリスクに対して、ISO27001、FedRAMP、FISMA、HIPAA等の認証のための外部監査の結果に基づいて、顧客への報告を行うよう計画しています。 ・IBM 社内監査にて体制、計画が作成され実施しています。 ・リスク評価や管理プロセスが整備されています。組織内では、役割と責任が定義され整備されています。 ・統制対象クラウド拠点の情報をウェブサイト上で公開しています。 ・利用者内部は、利用者にて整備を行っていただく前提です。 〈ご参考〉 ・IBM Cloud セキュリティガイドブック ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・SoftLayer Technologies, Inc. Infrastructure as a Service (IaaS) System 3 SOC 3 Report Relevant to the Security and Availability Principles ・ SOFTLAYER_US_SoftLayer SOC 1 2H 2017 Report ・A guide to IBM Bluemix resiliency and security	適合可能	文献[03]の473スライド目にて、共用VPNサービスのサーバーにつながらないとき、世界中のIBM Cloudのデータセンターやpopに接続することを確認した。 文献[03]の473スライド目にて、IBM Cloud側に何らかの問題があり、最寄りのリージョンへ接続できなかったり、自動的に転送されない場合の代替接続先があることを確認した。 文献[03]の473スライド目にて、IBM Cloudコンソールは、最寄りのリージョンで管理されているコンソールにつながるようになっていることを確認した。 文献[09]にて、SOC2の取得証明書を確認した。 なお、SOC2では、クラウドサービス固有のリスク対策について記載されていることを確認した。 文献[03]の232スライド目にて、IBM Cloud IaaS上に構築するOS、アプリケーションやデータの管理は利用者の責任範囲として規定されていることを確認した。	公開文書	文献[03] 文献[09]	SOC2 P24 Change Management	–	–	利用者は、自身のセキュリティ対策状況とクラウドサービスのセキュリティ対策状況を踏まえたうえで安全対策を講ずる必要がある。
統25	勘定系システムにおける共同センターとしてIBM Cloudを利用する場合の安全対策は利用者の責任範囲であるため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、確約事項及び契約内容を踏まえたうえで、共同センターを利用する金融機関間で適切な安全対策を講ずる必要がある。
統26	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、IBM Cloudにおいて障害が発生した場合に備え適切なリスク管理を行う必要がある。
実1	IBM Cloud ではパスワードの漏洩防止のために、非表示、非印字など必要な対策を講じています。	適合可能	文献[03]の227スライド目にて、二要素認証や認証統合サービスを、利用者にて取捨選択ののち構築もしくは設定できることを確認した。 文献[03]の342スライド目にて、パスワードは以下の制約があることを確認した。 ・半角文字のみ ・8文字以上31文字以下 ・スペース、?、[、]を除く特殊記号を利用可能 ・"password"という文字列を利用不可 ・IBMid自体を含めることは不可 ・苗字、名前を含めることは不可	公開文書	文献[03]	–	–	–	利用者は、自ら設定したパスワードを第三者に漏洩したり、第三者が類推しやすいパスワードを設定することを防ぐ必要がある。 利用者がIBM Cloud上で構築するアプリケーションやサービスで独自に用いるIDやパスワード等については、利用者が適切な対策を講じる必要がある。
実2	公衆通信網を通じた自動着信機能における相手端末確認は、業務の必要に応じて顧客が導入することとしており、対象外としました。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は公衆通信網を通じて自動着信端末に出力するアプリケーションを作成する場合は、相手先端末確認機能を設ける必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実3	・IBM Cloudデータ・セキュリティ クラウド上に配置するデータの重要性に応じて、暗号化の必要性の有無、配置場所、アクセス管理、バックアップデータの取り扱い方法等に対しては、お客様自身で対策を講じる必要があります。 ユーザー・アプリケーションで使用する業務データの管理は基本的にお客様にて実施いただきます。一部のデータベース・サービスでは DBMS が提供する暗号化機能を利用することができます。クラウド事業者としてサービス運用上必要となるデータのバックアップについてはクラウド事業者により取得され、すべて暗号化されインターネット から直接アクセスできない領域に保管されます。 <ご参考> ・IBMクラウド・セキュリティ ガイドブック ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[03]の334スライド目にて、IBM仮想マシン向けに設計されたデータ保護ソフト（Spectrum Protect Plus）にて、適切にデータを保護していることを確認した。 文献[03]の222スライド目にて、IBM データベース監査製品（Guardium）によるセンシティブ・データへのアクセスモニタリングを行っていることが確認できた。 文献[03]の222スライド目にて、データベース全体とバックアップデータは暗号化されており、暗号化キーは定期的に変更されていることが確認できた。 文献[03]の74スライド目にて、ファイルサーバーであるSAN（仮想サーバ）、内蔵HDD・SSD(物理サーバ）、IBM Cloud Block / File Storageは、暗号化されていることを確認した。 文献[01]の「4.8.2. データ保護」にて、データの所有権、管理責任は利用者であるお客様となることを確認できた。	公開文書	文献[01] 文献[03]	－	－	－	蓄積データの暗号化が必要な場合は、利用者のアプリケーションやサービスで実施する必要がある。 端末や周辺機器、アプリケーションが生成する一時データなどの管理は利用者の責任である。
実4	IBM Cloud への暗号化通信として、IBM Cloud IaaS側が管理している SSL-VPN/PPTP-VPN/IPsec-VPN サービスを利用することが可能です。この場合、利用者がIBM Cloud IaaS上に別途 VPN サーバを構築・ 運用する必要はありません。パブリック・ネットワークを使用せずにサーバにアクセスすることができるので、セキュアな通信が可能となります。 <ご参考> ・IBMクラウド・セキュリティガイドブック ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[03]の225スライド目にて、セキュアな通信プロトコルとしてSSL/TLSをサポートしていることを確認した。 文献[03]の245スライド目にて、IBM Cloudのカスタマーポータルや APIアクセスは、TLS1.2を利用して利用者端末との間で暗号化を行っており、そのために必要となるSSL証明書を維持・管理していることを確認した 文献[03]の126スライド目にて、運用管理用途で、IBM Cloud提供のSSL VPN接続サービスとIBM Cloud提供のIPsecVPN接続サービスを使用していることを確認した。	公開文書	文献[03]	－	－	－	利用者がIBM Cloud上で構築するアプリケーションやサービスで重要なデータを伝送する場合は、利用者がSSL暗号化を用いるなどの対策を行う必要がある。
実5	・IBM Cloudのクラウド・サービスにおいてデータの所有権および管理責任はお客様にあり、IBMの社員はアクセスできないようになっています（運用チームの担当員を除く）。 ・データアクセスにあたってはユーザーID/パスワードによる認証、ユーザー、グループ、IPホワイトリスト、ユーザーの役割に応じてデータの行および列のレベルで細かなアクセス制御が設定可能です。 <ご参考> ・IBMクラウド・セキュリティガイドブック ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[01]の「4.3.2. IBM Cloud プラットフォームにおけるデータ・セキュリティ」にて、クラウド事業者としてサービス運用上必要となるデータのバックアップについてはクラウド事業者により取得され、すべて暗号化されインターネットから直接アクセスできない領域に保管していることが確認できた。 文献[01]の「4.3.2. IBM Cloud プラットフォームにおけるデータ・セキュリティ」にて、IBM Cloud で使用する暗号鍵情報は、IBM Cloud プラットフォームの運用チームが管理しており、担当員以外によるアクセスはできないことを確認した。 文献[03]の222スライド目にて、ユーザーID/パスワードによる認証、ユーザー、グループ、ユーザーの役割に応じてデータの行および列のレベルで細かなアクセス制御を設定可能としていることを確認した。 文献[03]の210スライド目にて、IP ホワイトリストによるアクセス制御が可能であることを確認した。 文献[01]の「4.3.2. IBM Cloud プラットフォームにおけるデータ・セキュリティ」にて、外部からファイルシステムに直接的にアクセスできないようになっており、データを改ざんされるリスクは低くなっていることを確認した。 文献[01]の「4.8.2. データ保護」にて、データの所有権、管理責任は利用者であるお客様となる、と明記していることを確認できた。	公開文書	文献[01] 文献[03]	－	－	－	利用者に対するアクセス権限の設定は、SI事業者や利用者の管理者により適切に行われる必要がある。
実6	不良データの検出、除外機能は、業務の必要に応じて顧客が導入することとしており、対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	利用者がIBM Cloud上で構築するアプリケーションやサービスにおける不良データ検出機能は、それらのアプリケーションやサービス上で利用者が対策を行う必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実7	IBM Cloudでは以下の対応により伝送データの改ざん防止と検知を実施しています。 1.関連する 個別契約書 に記載された範囲において、IBM は、お客様がパブリック・ネットワークを介して「コンテンツ」を「クラウド・サービス」との間で安全に転送できるようにするために、公開表示または権限のない閲覧を意図しない「コンテンツ」をパブリック・ネットワークで転送する際に「コンテンツ」を暗号化し、暗号プロトコル (HTTPS、SFTP、および FTPS など) を使用可能にします。 2.IBM は、以下のことを行います。 1) 少なくとも年に 1 度、IBM の「クラウド・サービス」についてセキュリティーおよびプライバシーのリスク評価を実施する。 2)実稼働リリースの前およびその後毎年、侵入テストおよび脆弱性アセスメントを実施する（自動化されたシステムおよびアプリケーションのセキュリティー・スキャン、ならびに手動の倫理的ハッキングを含みます）。 3) 適格な独立した第三者に、侵入テストの実施を少なくとも年に 1 度依頼する。 4) 基盤となるコンポーネントのセキュリティー構成要件の遵守について、自動化された管理およびルーチン検証を実施する。 5) 関連するリスク、悪用の可能性、および影響に基づいて、特定された脆弱性またはセキュリティー構成要件の不遵守を修復する。 <ご参考> ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[01]の「4.3.2. IBM Cloud プラットフォームにおけるデータ・セキュリティ」にて、外部からファイルシステムに直接的にアクセスできないようになっており、データを改ざんされるリスクは低くなっていることを確認した。 文献[03]の225スライド目にて、セキュアな通信プロトコルとしてSSL/TLSをサポートしていることを確認した。 文献[03]の245スライド目にて、IBM Cloudのカスタマーポータルや APIアクセスは、TLS1.2を利用して利用者端末との間で暗号化を行っており、そのために必要となるSSL証明書を維持・管理していることを確認した。 文献[09]にて、SOC2の取得証明書を確認した。 なお、SOC2では、伝送データの改ざん検知策について記載されていることを確認した。	公開文書	文献[01] 文献[03] 文献[09]	SOC2 P24 Change Management	―	―	利用者がIBM Cloud上で構築するアプリケーションやサービスで重要なデータを伝送する場合は、利用者がSSL暗号化を用いるなどの対策を行う必要がある。
実8	IBM Cloudでは以下の対応により不正使用の防止が対応されています。 IBMか “「コンテンツ」に対するアクセスを必要とする場合、当該アクセスは、必要な最低限のレベルに制限されます。基盤となるコンポーネントに対する管理者としてのアクセス権 (特権的アクセス) を含む当該アクセス権は、個人用の、役割ベースのもので、職務分離の原則に従った、権限のある IBM 要員による承認および定期的な確認が行われることを条件とします。IBM は、特権的アクセス権の付帯する重複アカウントおよび休止アカウントを特定し、削除するための手段を維持管理します。また、アカウント所有者の離職にあたって、または権限のある IBM 要員 (アカウント所有者のマネージャーなど) の要求に応じて、当該アクセス権限を速やかに取り消します。 IBM Cloud ではIBM ID を使用してログイン認証を行います。ユーザーID とパスワード管理は IBM ID の方式に従いますが、このユーザーID に対して、管理コンソールへのアクセス許可を IP アドレスで制限したり、二要素認証機能を実装したりすることが可能です。また、「サポート」「デバイス」「ネットワーク」「セキュリティ」「サービス」「アカウント」からなる詳細な権限設定、およびサーバへの アクセス権限を管理することにより、きめ細やかなアクセス制御を実施することができます。 <ご参考> ・ クラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・ IBM クラウド・セキュリティガイドブック ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[01]の「4.6.1. IBM Cloud インフラストラクチャーにおける運用管理」にて、IBM Cloud インフラストラクチャーの運用チームや開発チームがIMS（情報管理システム） にログインするためには VPN および二要素認証の両方を必須としていることを確認した。 文献[01]の「4.5.2.3. IBM Cloud 上のアプリケーションのアクセス管理」にて、IBM Cloud は OAuth ベースの認証メカニズムを利用しており、お客様のアプリケーション開発者は自身が所属する IBM Cloud 組織・スペース・リソースグループのアプリケーションおよびサービス・インスタンスに対してのみアクセス権限を持っていることを確認した。 文献[03]の445スライド目にて、IBM CloudはIBM Cloud Identityを採用しており、多要素認証（FIDO, ワンタイムパスワード等）でセキュアなアクセスを可能としていることを確認した。	公開文書	文献[01] 文献[03]	―	―	―	利用者がIBM Cloud上で構築するアプリケーションやサービスで独自に用いる認証については、利用者が適切な本人確認機能を設ける必要がある。 特に、インターネットバンキングで用いる電子証明書の管理や認証方式の選択は利用者の責任である。
実9	IBM は、非アクティブ・セッションのタイムアウト、複数回連続でログインを試みて失敗したアカウントのロックアウト、強力なパスワードまたはパスフレーズによる認証を強制する技術的手段、ならびに当該パスワードおよびパスフレーズの安全な転送および保管を要求する手段を維持しています。 <ご参考> ・IBMクラウド・セキュリティガイドブック ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[02]の「5. アクセス、介入、転送、および分離の管理 f」にて、IBM は、非アクティブ・セッションのタイムアウト、複数回連続でログインを試みて失敗したアカウントのロックアウト、強力なパスワードまたはパスフレーズによる認証を強制する技術的手段、ならびに当該パスワードおよびパスフレーズの安全な転送および保管を要求する手段を維持していることを確認した。	公開文書	文献[02]	―	―	―	利用者がIBM Cloud上で構築するアプリケーションやサービスで独自に用いる認証については、利用者が適切な認証機構を用いる必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実10	IBM Cloudでは以下のポリシーに基づきアクセス履歴が管理されています。 IBM のポリシーは、クラウド・サービスのコンピューティング環境に対する管理を目的としたアクセスおよびこの環境内のアクティビティーについて、記録および監視すること、ならびに IBMの世界的な記録管理計画に従って、ログをアーカイブに保存および保持することを義務付けています。実稼働のクラウド・サービスに対する変更は、IBM の変更管理ポリシーに従って記録および管理されます。 <ご参考> ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[01]の「4.6.1. IBM Cloud インフラストラクチャーにおける運用管理」にて、IMS（情報管理システム） へのアクセスログは常に取得されており、それぞれの業務を遂行するにあたっての必要最低限のアクセス権限のみ付与されていることを確認した。 文献[01]の「4.6.3.2. 監査ログ」にて、IBM Cloud では、イベント管理(SIEM)ツールである IBM QRadar® を使用し、お客様のアプリケーション開発者・運用担当者の IBM Cloud プラットフォームに対するすべてのログイン認証に対して監査ログを作成していることを確認した。 また、IBM Cloud プラットフォーム は 同じく IBM QRadar® を使用して、IBM Cloud プラットフォーム上のアプリケーションが実行されているコンテナをホストするLinux システムに対する特権ユーザーのアクセスについても、監査ログを作成していることを確認した。 文献[02]の「5. アクセス、介入、転送、および分離の管理 h」にて、特権的なアクセスおよびアクティビティーが記録されたログは、IBM の世界的な記録管理計画に従って保存されていることを確認した。	公開文書	文献[01] 文献[02]	–	–	–	利用者は、自らが定めた監査ポリシーに従って記録されたログなどを、定期的に確認する必要がある。 利用者がIBM Cloud上で構築したアプリケーションやサービスのアクセス履歴については、利用者が適切にログの蓄積及び確認を行う必要がある。
実11	取引内容の制限機能は、業務の必要に応じて顧客が導入することとしており、対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	取引制限機能が必要なアプリケーションやサービスについては、利用者が対策する必要がある。
実12	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	取引制限機能が必要なアプリケーションやサービスについては、利用者が対策する必要がある。
実13	IBM は、個別契約書に明記されている場合、保管されている「コンテンツ」を暗号化します。「クラウド・サービス」に暗号鍵の管理が含まれる場合、IBMは、セキュリティー保護されたキーの生成、発行、配布、保管、ローテーション、失効、リカバリー、バックアップ、破棄、アクセスおよび使用に関する手続きを文書化し、維持管理します。 <ご参考> ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[03]の277スライド目にて、FIPS-140-2 Level3 認定のハードウェア・セキュリティ・モジュール (HSM) でプロビジョンした暗号鍵を保護していることを確認した。 文献[03]の277スライド目にて、保管した暗号鍵は、管理者あるいは開発者の権限を持つユーザーのみAPIで閲覧可能であることを確認した。 文献[01]の「4.3.2. IBM Cloud プラットフォームにおけるデータ・セキュリティ」にて、IBM Cloud で使用する暗号鍵情報は、IBM Cloud プラットフォームの運用チームが管理しており、担当員以外によるアクセスはできないようになっていることを確認した。 文献[01]の「4.4.2. IBM Cloud プラットフォームにおけるアプリケーション・セキュリティ」にて、アプリケーション自体のセキュリティを担保するのはお客様の責務となることを確認した。	公開文書	文献[01] 文献[03]	–	–	–	利用者は端末側で使用する暗号鍵が第三者に解読されたり漏洩することを防止する対策を講じる必要がある。 利用者がIBM Cloud上で構築したアプリケーションやサービスで独自に使用する暗号鍵の保護については、利用者が対策する必要がある。
実14	IBM Cloudでは以下の管理方法により外部ネットワークからの不正侵入に対する防止策を実施しています。 ・IBM Cloud Public および Dedicated では、ネットワークへのアクセスを制限するファイアーウォールが運用されており、ファイアーウォール上では侵入を防御するためのポリシーが有効化されています。 ・IBM Cloud IaaSは、プライベート・ネットワークを利用することができ、お客様ごとに専用のプライベートVLANが割り当てられ、プライベートIPアドレスを使ってインターネットに出ることなく通信できます。 ・Vyatta Gateway Applianceや専用ファイアーウォールを別途構成することで、パケット・フィルタリングを行います。 ・なお、アプリケーション自体のセキュリティを担保するのはお客様の責務となります。 <ご参考> ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[03]の271スライド目にて、IBM Cloud IaaSでは、IDSのネットワーク侵入検知機能を提供していることを確認した。(Windowsのみの機能) 文献[01]の「4.2.1.1. グローバルネットワーク」にて、IBM Cloud IaaSは、プライベート・ネットワークを利用することが可能で、お客様ごとに専用のプライベートVLANが割り当てられ、プライベートIPアドレスを使ってインターネットに出ることなく通信することが可能であることを確認した。同様に、パブリック・ネットワークを利用することが可能で、お客様ごとに専用のパブリックVLANが割り当てられ、パブリックIPアドレスを使ってインターネットに出ることなく通信することが可能であることを確認した。 文献[01]の「4.2.1.2. ファイアーウォール（パケット・フィルタリング）」にて、Vyatta Gateway Applianceや専用ファイアーウォールを別途構成することで、パケット・フィルタリングを行うことが可能であることを確認した。 文献[01]の「4.2.2.1. IBM Cloud プラットフォームに対するアクセス」にて、IBM Cloud Public および Dedicated では、ネットワークへのアクセスを制限するファイアーウォールが運用されており、ファイアーウォール上では侵入を防御するためのポリシーが有効化されていることを確認した。 文献[01]の「4.4.2. IBM Cloud プラットフォームにおけるアプリケーション・セキュリティ」にて、アプリケーション自体のセキュリティを担保するのはお客様の責務となることを確認した。	公開文書	文献[01] 文献[03]	–	–	–	ネットワークACLを用いて不正侵入を防止するためには、利用者が適切にネットワークACLを設定する必要がある。 ファイアウォールによる通信の送受信の確認や、WAFによるWebアプリケーションの保護などは、利用者が必要性を判断して構成する必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実15	IBM Cloudでは以下の管理方法により外部ネットワークからの不正侵入に対する防止策を実施しています。 ・IBM CloudではNetwork Operations Center(NOC)とSecurity Operation Center(SOC)のチームが、IBM Cloudの環境を24/365監視し、問題の特定およびインシデント対応を行っています ・アンチウィルスソフトやアンチスパイウェア対策ソフトウェアの導入、IDS機能をもつ対策ソフトウェアの導入、ログ監視や変更監視機能をもつソフトウェアを利用 ・IBM Cloud IaaSは、プライベート・ネットワークを利用することができ、お客様ごとに専用のプライベートVLANが割り当てられ、プライベートIPアドレスを使ってインターネットに出ることなく通信する。 ・Vyatta Gateway Applianceや専用ファイアーウォールを別途構成することで、パケット・フィルタリングを行う。 ・なお、アプリケーション自体のセキュリティを担保するのはお客様の責務となります。 <ご参考> ・ IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[03]の271スライド目にて、アンチウィルスソフトやアンチスパイウェア対策ソフトウェアの導入、IDS機能をもつ対策ソフトウェアの導入、ログ監視や変更監視機能をもつソフトウェアを利用できることを確認した。 文献[01]の4.2.1.1にて、IBM Cloud IaaSは、プライベート・ネットワークを利用することが可能で、お客様ごとに専用のプライベートVLANが割り当てられ、プライベートIPアドレスを使ってインターネットに出ることなく通信することが可能であることを確認した。同様に、パブリック・ネットワークを利用することが可能で、お客様ごとに専用のパブリックVLANが割り当てられ、パブリックIPアドレスを使ってインターネットに出ることなく通信することが可能であることを確認した。 文献[01]の4.2.1.2にて、Vyatta Gateway Applianceや専用ファイアーウォールを別途構成することで、パケット・フィルタリングを行うことが可能であることを確認した。 文献[03]の246スライド目にて、Network Operations Center(NOC)とSecurity Operation Center(SOC)のチームが、IBM Cloudの環境を24/365監視し、問題の特定およびインシデント対応の責任を負うことを確認した。 文献[01]の「4.4.2. IBM Cloud プラットフォームにおけるアプリケーション・セキュリティ」にて、アプリケーション自体のセキュリティを担保するのはお客様の責務となることを確認した。	公開文書	文献[01] 文献[03]	–	–	–	ネットワークACLを用いてアクセス可能な機器を必要最小限にするためには、利用者が適切にネットワークACLを設定する必要がある。
実16	・IBM Cloud では、Network Operations Center (NOC) および Security Operations Center (SOC) が、サービス基盤を監視し、インシデントの特定、対応、解決を行います。NOC および SOC により、IBM Cloud は24時間365日の監視を行います。 <ご参考> ・技術よりな人が最初に読む：IBMCloud柔らか層本. ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・IBMクラウド・セキュリティガイドブック ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[01]の「4.6.3.2. 監査ログ」にて、IBM Cloud では、イベント管理(SIEM)ツールであるIBM QRadar® を使用し、お客様のアプリケーション開発者・運用担当者のIBM Cloud プラットフォームに対するすべてのログイン認証に対して監査ログを作成していることを確認した。 文献[01]の「4.2.2.3. DDoS対応」にて、ネットワーク装置のログはセキュリティ情報およびイベント管理（SIEM）ツール IBM QRadarを使い、統合的な監視を実施していることを確認した。	公開文書	文献[01]	–	–	–	利用者がIBM Cloud上で構築したアプリケーションやサービスに対する不正アクセスの監視については、利用者が対策する必要がある。
実17	異常な取引状況を把握する機能は、業務の必要に応じて顧客が導入することとしており、対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	異常な取引状況を把握する機能が必要なアプリケーションやサービスについては、利用者が対策する必要がある。
実18	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	異例取引の監視機能が必要なアプリケーションやサービスについては、利用者が対策する必要がある。
実19	・IBM は、コンピューターのセキュリティー・インシデントの取り扱いについての NIST ガイドラインラインに合致する、文書化されたインシデント対応ポリシーを維持管理してこれに従い、本契約のデータ漏えいの通知に関する条件を遵守します。 ・IBM は、IBM が認知した「コンテンツ」の不正アクセスおよび不正使用 (セキュリティー・インシデント) を調査し、「クラ ウド・サービス」の範囲内で、適切な対応プランを定義し実行します。利用者は、テクニカル・サポート要求を提出すること によって、脆弱性またはインシデントの疑いについて IBM に通知することができます。 ・IBM は、利用者に影響を及ぼすと認知するか、そのおそれがあると合理的に判断したときには、遅滞なく利用者に通知しま す。IBM は、当該セキュリティー・インシデントならびに IBM による修復および回復作業の状況について合理的に要求され た情報を利用者に提供します。 <ご参考> ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[09]にて、ISO27001の取得証明書を確認した。 ISO27001の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 - A.16.1.1 責任及び手順 情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立しなければならない。 - A.16.1.5 情報セキュリティインシデントへの対応 情報セキュリティインシデントは、文書化した手順に従って対応しなければならない。 - A.16.1.6 情報セキュリティインシデントからの学習 情報セキュリティインシデントの分析及び解決から得られた知識は、インシデントが将来起こる可能性又はその影響を低減するために用いなければならない。 文献[02]の「3. セキュリティー・インシデント a」にて、IBM は、コンピューターのセキュリティー・インシデントの取り扱いについての NIST ガイドラインに合致する、文書化されたインシデント対応ポリシーを維持管理してこれに従い、本契約のデータ漏えいの通知に関する条件を遵守していることを確認した。 文献[02]の「3. セキュリティー・インシデント b」にて、IBM は、IBM が認知した「コンテンツ」の不正アクセスおよび不正使用 (セキュリティー・インシデント) を調査し、「クラウド・サービス」の範囲内で、適切な対応プランを定義し実行することを確認した。 文献[02]の「3. セキュリティー・インシデント c」にて、IBM は、IBM が認知した、または IBM が合理的に疑うお客様に影響を及ぼすセキュリティー・インシデントについて、お客様にすみやかに通知することを確認した。 文献[02]の「3. セキュリティー・インシデント c」にて、IBM は、当該セキュリティー・インシデントに関し合理的に要求された情報ならびに IBM による修復および回復作業の状況について、お客	公開文書	文献[02] 文献[09]	ISO27001 A.16.1.1 A.16.1.5 A.16.1.6 SOC2 P20 Intrusion Detection	–	–	利用者がIBM Cloud上で構築したアプリケーションやサービスに対する不正アクセスについては、利用者が対応策及び復旧策を講じる必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実20	・IBM Cloud の環境にデプロイしたサービスおよび利用者のコンテンツ（利用者のアプリケーションおよびデータを含みます。）は、利用者ご自身で管理いただきます。 ・IBM は、IBM Cloud IaaS の責任範囲において、以下の実施を含む脆弱性対策を行います。 － インターネット接続されているすべての機器に対する脆弱性スキャン － 定期的なセキュリティーおよびプライバシーのリスク評価の実施 － 適格な独立した第三者による、侵入テストの実施 － 実稼働リリースの前およびその後毎年、侵入テストおよび脆弱性アセスメントを実施 － 関連するリスク、悪用の可能性、および影響に基づいて、特定された脆弱性またはセキュリティー構成要件の不遵守の修復 <ご参考> ・技術よりな人が最初に読む：IBMCloud柔らか層本 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・IBMクラウド・セキュリティガイドブック ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[03]の271スライド目にて、アンチウィルスソフトやアンチスパイウェア対策ソフトウェアの導入、IDS機能をもつ対策ソフトウェアの導入、ログ監視や変更監視機能をもつソフトウェアを利用できることを確認した。 文献[01]の「4.4.2. IBM Cloud プラットフォームにおけるアプリケーション・セキュリティ」にて、アプリケーション自体のセキュリティを担保するのはお客様の責務となることを確認した。	公開文書	文献[01] 文献[03]	－	－	－	利用者がIBM Cloud上で構築したアプリケーションやサービスに対する不正プログラムへの防御対策については、利用者が対応を講じる必要がある。
実21	・IBM Cloud では、Network Operations Center (NOC) および Security Operations Center (SOC) が、サービス基盤を監視し、インシデントの特定、対応、解決を行います。NOC および SOC により、IBM Cloud は24時間365日の監視を行います。 <ご参考> ・技術よりな人が最初に読む：IBMCloud柔らか層本 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・IBMクラウド・セキュリティガイドブック ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[03]の271スライド目にて、アンチウィルスソフトやアンチスパイウェア対策ソフトウェアの導入、IDS機能をもつ対策ソフトウェアの導入、ログ監視や変更監視機能をもつソフトウェアを利用できることを確認した。 文献[03]の297スライド目にて、IBM Cloud IaaSでは、Windowsサーバー用に不正侵入防御のサービスが提供されていることを確認した。 また、アンチウィルス・アンチスパイウェア・IDSの機能が利用でき、それぞれについてIBM Cloud コンソールからログを確認できることを確認した。 文献[01]の「4.4.2. IBM Cloud プラットフォームにおけるアプリケーション・セキュリティ」にて、アプリケーション自体のセキュリティを担保するのはお客様の責務となることを確認した。	公開文書	文献[01] 文献[03]	－	－	－	利用者がIBM Cloud上で構築したアプリケーションやサービスに対する不正プログラムの検知対策については、利用者が対応を講じる必要がある。
実22	・IBMは、コンピューターのセキュリティー・インシデントの取り扱いについてのNISTガイドラインに合致する、文書化されたインシデント対応ポリシーを維持管理してこれに従い、本契約のデータ漏えいの通知に関する条件を遵守します。 ・IBMは、IBMが認知した「コンテンツ」の不正アクセスおよび不正使用（セキュリティー・インシデント）を調査し、「クラウド・サービス」の範囲内で、適切な対応プランを定義し実行します。利用者は、テクニカル・サポート要求を提出すること によって、脆弱性またはインシデントの疑いについてIBMに通知することができます。 ・IBMは、利用者に影響を及ぼすと認知するか、そのおそれがあると合理的に判断したときには、遅滞なく利用者に通知します。IBMは、当該セキュリティー・インシデントならび "にIBMによる修復および回復作業の状況について合理的に要求された情報を利用者に提供します。 <ご参考> ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[09]にて、ISO27001の取得証明書を確認した。 ISO27001の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － A.16.1.1 責任及び手順 情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立しなければならない。 － A.16.1.5 情報セキュリティインシデントへの対応 情報セキュリティインシデントは、文書化した手順に従って対応しなければならない。 － A.16.1.6 情報セキュリティインシデントからの学習 情報セキュリティインシデントの分析及び解決から得られた知識は、インシデントが将来起こる可能性又はその影響を低減するために用いなければならない。	公開文書	文献[09]	ISO27001 A.16.1.1 A.16.1.5 A.16.1.6	－	－	利用者がIBM Cloud上で構築したアプリケーションやサービスに対する不正プログラムの被害時対策については、利用者が対応を講じる必要がある。
実23	・利用者は、構築された利用者システムにおける正確かつ安全に運用するマニュアルの整備を実施する必要があります。 ・本部・営業店等設置の端末機操作についてのマニュアルについては利用者にて対応していただく。 ・IBM Cloud の運用管理規定ならびに体制は、内部文書にて定義されています。 <ご参考> ・IBMクラウド・サービスのデータのセキュリティおよびプライバシーの原則： https://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp ・IBM Cloud のコンプライアンス： https://console.bluemix.net/docs/security/compliance.html#compliance ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[02]の「4. 物理的セキュリティーおよび入場管理 b」にて、正式な離職手続き（アクセス制御リストからの速やかな削除、物理的なアクセス・バッジの返却などを含みますが、これらに限定されません。）を文書化していることを確認した。 文献[02]の「5. アクセス、介入、転送、および分離の管理 d」にて、セキュリティー保護されたキーの生成、発行、配布、保管、ローテーション、失効、リカバリー、バックアップ、破棄、アクセス、および使用に関する手続きを文書化していることを確認した。	公開文書	文献[02]	－	－	－	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実24	・利用者は、構築された利用者システムにおける正確かつ安全に運用するマニュアルの整備を実施する必要があります。 ・利用者は、実装するアプリケーションの障害対策・災害対策に関する対応を実施する必要があります。 ・利用者は、提供する複数のリージョンを利用し、可用性を重視したアーキテクチャー設計/構築することにより、ビジネス継続性を実現することが可能です。 ・障害や災害に備えてIMS機能によりシステム構成情報を管理しており、遠隔バックアップを随時取得しています。 ・バックアップからの復旧はスクリプトによる自動化を図っており、手順は簡略化されています。 ・復旧操作の訓練は定期的に実施しています。 ・なお、IBM Cloud IaaSのセキュリティ管理は、ISO27001 を基準としたIBM Cloud Security Policy とNIST 800-53 framework をベースとしたUS 政府標準に準拠して運用されています。 〈ご参考〉 ・IBM Cloud セキュリティガイドブック ・IBMクラウド・サービスのデータのセキュリティおよびプライバシーの原則：https://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp ・IBM Cloud のコンプライアンス：https://console.bluemix.net/docs/security/compliance.html#compliance ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[04]の「3.2 可用性 SLA」にて、IBM Cloud IaaSのSLAとして、ハードウェア障害時および計画的なハードウェア・アップデートを実施する場合は、ダウンタイムを最小限に抑えるようにし、2時間以内の対応完了が定められていることを確認した。 文献[03]の53スライド目にて、パブリック、プライベート、ハイブリッドの各クラウドにエンタープライズ・レベルの災害復旧と事業継続性を提供することを確認した。 文献[03]の403スライド目にて、障害時の対応フローおよび役割分担を、①運用管理の責任範囲がIBM Cloudにある場合、②運用管理の責任範囲が利用者にある場合、③監視、対応依頼の責任範囲のみ利用者にある場合、の3つのパターンに分けて記載されていることを確認した。 文献[07]の「6. サービスの感染性および可用性管理 d」にて、各「クラウド・サービス」は、事業継続性および災害復旧の要件について、文書化されたリスク管理ガイドラインに従って個別に評価されることを確認した。 文献[07]の「6. サービスの感染性および可用性管理 d」にて、各IBM「クラウド・サービス」には、当該リスク・アセスメントで保証される範囲において、業界標準の実務に合致する事業継続性および災害復旧の計画が付帯することを確認した。当該計画は、個別に定義され、文書化され、維持され、毎年検証されることを確認できた。 文献[07]の「6. サービスの感染性および可用性管理 d」にて、「クラウド・サービス」のリカバリー・ポイントおよびリカバリー時間の達成目標が提供される場合、「クラウド・サービス」のアーキテクチャーおよび使用目的を考慮して設定され、関連のTD（取引文書）に記載されることを確認した。	公開文書	文献[03] 文献[04] 文献[07]	–	–	–	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実25	・IBM Cloud 上に構築するOS、アプリケーションやデータの管理は利用者の責任範囲として規定されています。 ・利用者のシステム管理者によるアクセスはIMS機能が提供するポータルを経由することとし、利用者の管理責任者にマスターIDを交付しています。利用者側のアクセス権限管理やパスワードポリシー設定は当該管理者が行います。利用者システム管理者のアクセスはIMS機能によりログが取得されます。 ・IBM Cloud の運用、開発は、業務を遂行するにあたっての必要最低限のアクセス権限のみ付与されています。 ・IBM Cloud 要員のアクセス権限は担当職務に応じて付与され、3か月毎に棚卸を行っています。アクセスログはIMS、コンソールあるいはルータ等の各種機能により取得し、リスクに応じて承認手続とログの照合が行われます。 ・利用者は、実装するアプリケーションについて、システムへのアクセス制御に関する対応を実施する必要があります。 〈ご参考〉 ・IBM Cloud セキュリティガイドブック：https://www.ibm.com/downloads/cas/DG5Q0DRA ・技術よりな人が最初に読む:IBMCloud柔らか層本. ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[01]の「4.6.3.2. 監査ログ」にて、IBM Cloud では、イベント管理(SIEM)ツールである IBM QRadar® を使用し、お客様のアプリケーション開発者・運用担当者の IBM Cloud プラットフォームに対するすべてのログイン認証に対して監査ログを作成していることを確認した。 また、IBM Cloud プラットフォーム は 同じく IBM QRadar® を使用して、IBM Cloud プラットフォーム上のアプリケーションが実行されているコンテナをホストするLinux システムに対する特権ユーザーのアクセスについても、監査ログを作成していることを確認した。 文献[01]の「4.5.1. IBM Cloud インフラストラクチャーにおける ID・アクセス管理」にて、「サポート」「デバイス」「ネットワーク」「セキュリティ」「サービス」「アカウント」からなる詳細な権限設定、およびサーバーへのアクセス権限を管理することにより、きめ細やかなアクセス制御を実施することができることを確認した。 文献[01]の「4.5.2.1. IBM Cloud プラットフォーム利用ユーザーの ID 管理」にて、お客様のアプリケーション開発者は自身が所属する IBM Cloud 組織・スペース・リソースグループのアプリケーションおよびサービス・インスタンスに対してのみアクセス権限を持つことを確認できた。 なお、IBM Cloud 組織の管理者は管理コンソールを使用して、組織/リソース・グループ内の IBM Cloud ユーザーおよびその役割を管理できることを確認した。 文献[01]の「4.5.2.2. IBM Cloud プラットフォームへのアクセス管理」にて、IBM Cloud 運用チーム内では職務分離ガイドラインに従い、運用チームに細かいアクセス特権を割り当てることを確認した。そのため、運用チームは作業の実行に必要なアクセス権限のみを持つことを確認した。 文献[01]の「4.6.1. IBM Cloud インフラストラクチャーにおける運用管理」にて、IMS（情報管理システム）へのアクセスログは常に取得されており、それぞれの業務を遂行するにあたっての必要最低限のアクセス権限のみ付与されることを確認した。	公開文書	文献[01]	–	–	–	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。 利用者は、利用者自身のユーザーによるアクセスを制御し、それらアクセスを適切に確認する責任を負う。
実26	・IBM 社員は、ビジネス・コンダクト・ガイドラインにて、情報セキュリティー・ポリシー、コントロールおよびプロセスに従うことが義務付けられています。これには、パスワードを他者に教えてはいけないことが含まれます。 ・ISO 27001 A.9.2 より、利用者の秘密認証情報の管理は適切に行われています。 ・利用者は、アクセスに利用するIDのパスワード、利用者アプリケーションで利用するパスワードの管理を対応頂きます。 ・パスワードの漏洩防止　BCGを年一回certify研修しています。 〈ご参考〉 ・IBM Cloudのコンプライアンス対応：https://www.ibm.com/cloud-computing/bluemix/ja/compliance ・IBMビジネス・コンダクト・ガイドライン：https://www.ibm.com/multimedia/portal/V228557E52091P96/BCG_accessible_Japanese_2019IBM.pdf ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	インタビューにて、IBMビジネス・コンダクト・ガイドラインに従ったセキュリティ研修を、IBM社員向けに毎年行っていることを確認した。 文献[09]にて、SOC2の取得証明書を確認した。 なお、SOC2では、パスワードの漏洩防止処置について記載されていることを確認した。 文献[06]にて、IBMの所有か他社の所有かに関係なく、専有情報および機密情報の不注意による情報漏洩を避けるように注意しなければならないこと、決してパスワードを他者に教えてはいけないことを確認した。 文献[03]の342スライド目にて、パスワードは以下の制約があることを確認した。 ・半角文字のみ ・8文字以上31文字以下 ・スペース、?、{、}を除く特殊記号を利用可能 ・“password”という文字列を利用不可 ・IBMid自体を含めることは不可 ・苗字、名前を含めることは不可	要NDA	文献[03] 文献[06] 文献[09]	SOC2 P18 Logical Security	IBMビジネス・コンダクト・ガイドラインに従ったセキュリティ研修を、IBM社員向けに毎年行っている。	–	利用者は、承認されていない第三者にパスワードが開示されないようにする責任と、事実上推測できない十分な強度を備えたパスワードを選択する責任を負う。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実27	・利用者のシステム管理者のアクセス権限は利用者の管理責任者が付与、見直しを行うこととしています。 ・IBM Cloud要員は担当職務の必要に応じてアクセス権限が付与され、異動時や契約要員の業務終了時は速やかに権限変更や削除が行われます。権限の棚卸しは3か月毎に行われます。 ・利用者は、実装するアプリケーションについて、システムへのアクセス制御に関する対応を実施する必要があります。 〈ご参考〉 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	インタビューにて、IBM社員のアクセス権限は担当職務に応じて付与され、3か月毎に棚卸を行っていることを確認した。 文献[01]の「4.5.2.1. IBM Cloud プラットフォーム利用ユーザーの ID 管理」にて、お客様のアプリケーション開発者は自身が所属する IBM Cloud 組織・スペース・リソースグループのアプリケーションおよびサービス・インスタンスに対してのみアクセス権限を持つことを確認できた。 なお、IBM Cloud 組織の管理者は管理コンソールを使用して、組織/リソース・グループ内の IBM Cloud ユーザーおよびその役割を管理できることを確認した。	要NDA	文献[01]	―	IBM社員のアクセス権限は担当職務に応じて付与され、3か月毎に棚卸を行っている。	―	利用者がIBM Cloud上で構築する環境でのアクセス権限の付与、見直し手続きについては、利用者が明確にする必要がある。
実28	データの入力は利用者により管理されており、対象外とします。	対象外	金融機関内部の統制のため対象外	―	―	―	―	―	利用者は、データファイルの授受、保管方法を定める必要がある。
実29	データの入力は利用者により管理されており、対象外とします。	対象外	金融機関内部の統制のため対象外	―	―	―	―	―	利用者は、データファイルの修正及び管理方法を定める必要がある。
実30	・利用者は、実装するアプリケーションで利用する暗号鍵管理の対応を実施する必要があります。 ・IBM は、TD(個別契約書) に明記されている場合、保管されている「コンテンツ」を暗号化します。「クラウド・サービス」に暗号鍵の管理が含まれる場合、IBM は、セキュリティー保護されたキーの生成、発行、配布、保管、ローテーション、失効、リカバリー、バックアップ、破棄、アクセス、および使用に関する手続きを文書化し、維持管理します。 〈ご参考〉 ・IBM Cloud カタログ：https://console.bluemix.net/catalog/ ・技術よりな人が最初に読む IBM Cloud柔らか層本 ・クラウト゛・サーヒ゛スのテ゛ータのセキュリティーおよひ゛フ゜ライハ゜シーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[03]の277スライド目にて、鍵の生成、保管、取得、および管理のための、アプリケーションから独立したクラウド・ベースの鍵管理していることを確認した。 なお、保管した暗号鍵は、管理者あるいは開発者の権限を持つユーザーのみAPIで閲覧可能となっていることを確認した。 文献[02]の「5. アクセス、介入、転送、および分離の管理 d」にて、「クラウド・サービス」に暗号鍵の管理が含まれる場合、IBM は、セキュリティー保護されたキーの生成、発行、配布、保管、ローテーション、失効、リカバリー、バックアップ、破棄、アクセス、および使用に関する手続きを文書化し、維持管理していることを確認した。	公開文書	文献[02] 文献[03]	―	―	―	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実31	IBM Cloud のオペレーターはCloud Support AcademyのNew Hire Trainingを必須で受講するよう指示されています。 〈ご参考〉 Cloud Support Academy	適合可能	文献[01]の3.3にて、IBM 社員へのセキュリティ教育の徹底等は全世界で同一レベルのものが施されており、監査レポートでも明らかにしていることを確認した。 文献[01]の4.6.1にて、IBM Cloud インフラストラクチャーのセキュリティ管理は、ISO27001 を基準とした IBM Cloud Security Policy と NIST 800-53 framework をベースとした US 政府標準に準拠して運用されていることを確認した。 なお、IBM Cloud インフラストラクチャーの作業員は、この基準に従って定期的にセキュリティ教育を受けていることを確認した。 NDA文献[N03]及びインタビューにて、オペレーターは、IBM Cloudのオペレーションに係るトレーニングを定期的に受講していることを確認した。	要NDA	文献[01]	―	―	NDA文献[N03]	利用者は、IBM Cloudに関わる人材の情報セキュリティ教育を実施する必要がある。
実32	IBM Cloud 環境において、プラットフォームや各サービスを稼働させるためOSやミドルウェアはマネージド・サービスとして提供されており、ウィルス対策ソフトウェアの最新パターン・ファイル適用、OS アップデート等の維持・運用はすべてIBMが実施しています。 〈ご参考〉 ・IBMクラウド・セキュリティガイドブック ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[09]にて、ISO27001の取得証明書を確認した。 ISO27001の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － A.12.2.1 マルウェアに対する管理策 マルウェアから保護するために、利用者に適切に認識させることと併せて、検出、予防及び回復のための管理策を実施しなければならない。 － A.12.3.1 情報のバックアップ 情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査しなければならない。 文献[01]の「4.4.2. IBM Cloud プラットフォームにおけるアプリケーション・セキュリティ」にて、IBM Cloud プラットフォーム において、プラットフォームや各サービスを稼働させるためのOSやミドルウェアはマネージド・サービスとして提供されており、ウィルス対策ソフトウェアの最新パターン・ファイル適用、OS アップデート等の維持・運用はすべてIBM が実施することを確認した。 文献[03]の271スライド目にて、アンチウィルスソフトやアンチスパイウェア対策ソフトウェア、IDS機能をもつ対策ソフトウェアを導入することを確認した。	公開文書	文献[01] 文献[03] 文献[09]	ISO27001 A.12.2.1 A.12.3.1	―	―	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実33	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	―	―	―	―	―	利用者は、回線接続契約に際し、接続条件を明確にする必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実34	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、契約や規定により接続相手先の本人確認や端末確認の方法を明確にし、適切な管理を行う必要がある。
実35	IBM は、新規採用者全員について、自社の標準の必須の雇用検証要件を維持し、これに従います。また、当該要件の遵守を IBM の完全子会社にも拡大して適用します。IBM の社内プロセスおよび手続きに従って、これらの要件は定期的に見直されます。また雇用確認要件には、犯罪歴の確認、身元確認の証拠および IBM が必要とみなすその他の確認が含まれます。IBM の各法人は、現地の法律に基づいて許容され、かつ適用可能な範囲で、適宜、その採用プロセスに上記の要件を組み込む責任を負います。 また、データセンターのオペレーターはその役割に基づいてアクセス権を付与しています。 アクセスコントールに関するプロセルルールを規定しています。 〈ご参考〉 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance ・Core Controls for C3 Compliance Program	適合可能	NDA文献[N04]にて、アクセスコントロールに関するルールが定められていることを確認した。 文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 9.2.3 特権的アクセス権の管理 JIS Q 27002 の9.2.3 に定める管理策並びに付随する実施の手引及び関連情報を適用する。 文献[02]の「4. 物理的セキュリティーおよび入場管理 b」データセンターおよび管理エリアに入場するためのアクセス・バッジの使用は、使用の記録が取られ、当該記録は 1 年以上保存されることを確認した。	要NDA	文献[02] 文献[09]	ISO27017 9.2.3	–	NDA文献[N04]	利用者は、IBM Cloudで割り当てられたリソースの運用管理時、及びIBM Cloud上で構築する環境の運用管理時に、オペレーターの資格確認を運用管理者が行う必要がある。また、例外的に開発担当者等にオペレーション資格を付与するときは、運用管理者が承認する必要がある。オペレータの資格確認の方法の例には次のものがある。 例）制服の着用 腕章の着用 名札の着用
実36	IBM Cloud では以下の対応によりオペレーション管理を実施しています。 ・利用者からの問合せ等はIMS機能によりチケットとして通知され、専任の担当者がアサインされ、終了までの進捗を管理します。 ・利用者からの質問や要望に対する回答や、メニューから選択できない注文、IBM Cloud によるメンテナンスの通知などはすべてチケットを通してやり取りされます。チケットの内容は管理ポータルで確認できます。また、起票者に加えて任意のメンバーに、メールで更新通知をするように設定できます。 ・利用者は、実装するアプリケーションに関するオペレータの対策を実施する必要があります。 ・オペレーションのための手順は文書化され、適切な管理層の認可に基づいて訓練された実務管理者によって実施されます。 〈ご参考〉 ・技術よりな人が最初に読む IBM Cloud柔らか層本 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・Core Controls for C3 Compliance Program	適合可能	文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 12.5.1 運用システムに関わるソフトウェアの導入 JIS Q 27002 の12.5.1 に定める管理策及び付随する実施の手引を適用する。 文献[09]にて、SOC2の取得証明書を確認した。 なお、SOC2では、オペレーションの依頼・承認手続きについて記載されていることを確認した。 文献[02]の「4. 物理的セキュリティーおよび入場管理 c」にて、データセンター施設、またはデータセンター内の管理エリアに入場する一時的な許可を正式に付与されたいかなる個人も、当該施設に入場する際に登録され、登録時に身分証明書の提示が義務付けられ、権限ある要員が付き添うことを確認した。 文献[02]の「4. 物理的セキュリティーおよび入場管理 c」にて、搬出・搬入を含む、入場のための一時的な許可は、事前の計画および権限ある承認を必要とすることを確認した。	公開文書	文献[02] 文献[09]	ISO27017 12.5.1	–	–	利用者は、オペレーションの依頼・承認移管する手続きを定める必要がある。
実37	IBM Cloud環境では以下のような不正のできないオペレーション体制となっています。 データセンターおよびデータセンター内の管理エリアへのアクセスは、職務別に制限され、権限ある承認が必要になります。 データセンターおよび管理エリアに入場するためのアクセス・バッジの使用は、使用の記録が取られ、当該記録は 1 年以上保存されます。管理されたデータセンター・エリアへのアクセス権限を有する従業員が離職するにあたって、IBM は、当該従業員のアクセス権限を取り消します。IBM は、文書化された正式な離職手続き (アクセス制御リストからの速やかな削除、物理的なアクセス・バッジの返却などを含みますが、これらに限定されません。) に従います。また、運用オペレーションも職務別に制限されています。 データセンター施設、またはデータセンター内の管理エリアに入場する一時的な許可を正式に付与されたいかなる個人も、当該施設に入場する際に登録され、登録時に身分証明書の提示が義務付けられ、権限ある要員が付き添います。搬出・搬入を含む、入場のための一時的な許可は、事前の計画および権限ある承認を必要とします。 〈ご参考〉 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・Core Controls for C3 Compliance Program	適合可能	文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 12.1.2 変更管理 JIS Q 27002 の12.1.2 に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。 文献[09]にて、SOC2の取得証明書を確認した。 なお、SOC2では、誤操作・不正使用を防止するためのオペレーション実行体制について記載されていることを確認した。 文献[01]の「3.3. 外部委託管理」にて、データセンターはデータセンター事業者への委託となっているため、データセンター自体の管理運用、入退室管理等については委託先であるデータセンター事業者に託しているが、外部監査などの第三者機関による監査により、管理状況は全て透明性を以って開示しており、日本の上場企業の要求に十分に耐えうるサービスを提供していることを確認した。 文献[03]の228スライド目にて、運用は人手を介さないよう極力自動化していることを確認した。 文献[01]の「4.1.1. IBM Cloud インフラストラクチャーにおける物理セキュリティ」にて、お客様ごとのネットワーク構成やネットワーク設定などの作業は全て内部システムにより自動化されており、属人的な作業を可能な限り廃していることを確認した。 文献[03]の239スライド目にて、NWプロビジョニングもサーバープロビジョニングもすべて自動化していることを確認した。 文献[03]の233スライド目にて、IBM Cloud IaaSにおける利用者・クラウド業者の責任分界点を明	公開文書	文献[01] 文献[02] 文献[03] 文献[09]	ISO27017 12.1.2 SOC2 P28 People Organization and Administration	–	–	利用者は、オペレーターチームの編成及びオペレーション手順を定める必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実38	IBM Cloud環境では以下の規定により全てのオペレーション作業の記録が保存されます。 特権的なアクセスおよびアクティビティーが記録されたログは、IBM の世界的な記録管理計画に従って保存されます。IBM は、当該ログについて、不正アクセス、変更および偶発的または故意による破壊から保護することを目的として設計された 対策を維持します。 〈ご参考〉 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則	適合可能	文献[02]の「5.アクセス、介入、および分離の管理 g」にて、IBMは、特権的アクセス権の使用をモニターし、以下を目的として策定された、セキュリティ情報およびイベント管理の対策を維持することを確認した。 ・不正アクセスおよび不正なアクティビティーの特定 ・タイムリーかつ適切な対応の促進 ・文書化されたIBMポリシーへの準拠に関する社内監査および独立した第三者による監査の実施 文献[02]の「5.アクセス、介入、および分離の管理 h」にて、特権的なアクセスおよびアクティビティーが記録されたログは、IBM の世界的な記録管理計画に従って保存されることを確認した。なお、IBM は、当該ログについて、不正アクセス、変更、および偶発的または故意による破壊から保護することを目的として設計された対策を維持することを確認した。	公開文書	文献[02]	―	―	―	利用者は、オペレーション実行時の運行状況を確認し、オペレーションを記録する必要がある。
実39	IBM Cloud環境では以下のポリシーによりデータファイルのバックアップを確保しています。 ・IBM Cloud上のデータに関してのバックアップはお客様の責務となりますが、IBM Cloudとしては各種バックアップ取得のためのツールを提供しており、それらを活用してバックアップ取得が可能です。 ・クラウド事業者として必要なバックアップはIBM Cloudとして取得しています。また、バックアップ・マネージド・サービスのようなバックアップ運用サービスも契約することが可能です。 〈ご参考〉 ・IBM クラウド・セキュリティガイドブック	適合可能	文献[01]の「3.2. データ管理」にて、クラウド事業者としてサービス運用上必要となるデータのバックアップについてはクラウド事業者により取得され、すべて暗号化されインターネットから直接アクセスできない領域に保管されていることを確認した。 文献[03]の330スライド目にて、IBM Cloud が提供するバックアップ方式と、それぞれの方式に対するバックアップの対象を明示しており、用途に応じて適したものを選択するようにしていることを確認した。 文献[01]の「4.3.2. IBM Cloud プラットフォームにおけるデータ・セキュリティ」にて、クラウド上に置くデータの重要性に応じて、暗号化の必要性の有無、配置場所、アクセス管理、バックアップデータの取り扱い方法等に対しても、利用者自身で対策を講じる必要があることを確認した。	公開文書	文献[01] 文献[03]	―	―	―	利用者は、必要に応じて自社でのデータの抽出及びバックアップの実行を選択する必要がある。
実40	・IBM Cloud 環境では、プラットフォームや各サービスを稼働させるためのOSやミドルウェアはマネージド・サービスとして提供されており、ウィルス対策ソフトウェアの最新パターン・ファイル適用、OS アップデート等の維持・運用はすべて IBM が実施しています。 ・IBM Cloud環境で構築されたユーザープログラムの管理については利用者側で実施する必要があります。利用者アプリケーションに対する継続的な監視、テスト、監査の実施、インシデント発生時の対応は、利用者にて責任を負います。こうしたアプリケーションの保護はIBM Cloudが提供するサービスを利用するあるいは利用者自身がソフトウェアを持ち込んで実装することにより実現します。 〈ご参考〉 ・IBM クラウド・セキュリティガイドブック	適合可能	文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 9.4.5 プログラムソースコードへのアクセス制御 JIS Q 27002 の9.4.5 に定める管理策及び付随する実施の手引を適用する。 文献[01]の「4.3.2. IBM Cloud プラットフォームにおけるデータ・セキュリティ 」にて、IBM Cloud はプラットフォームとしてコミュニティベースの PaaS 実行基盤である Cloud Foundry を採用しており、IBM Cloud 上で稼働する各アプリケーション・インスタンスはコンテナ上で実行されること、外部からファイルシステムに直接的にアクセスできないようになっており、データを改ざんされるリスクは低くなっていることを確認した。 文献[03]の213スライド目にて、Cloudant NoSQL DB（マネージド・サービスとしてIBMが提供するドキュメント型のNoSQL DB）上で、データはバージョン管理(MVCC)されており、更新の順番を保証していることを確認した。	公開文書	文献[01] 文献[03] 文献[09]	ISO27017 9.4.5	―	―	利用者は、プログラムファイルの管理方法を定める必要がある。
実41	IBM Cloud環境では以下のポリシーによりプログラムファイルのバックアップを確保しています。 ・IBM Cloud上のプログラムに関してのバックアップはお客様の責務となりますが、IBM Cloudとしては各種バックアップ取得のためのツールを提供しており、それらを活用してバックアップ取得が可能です。 ・クラウド事業者として必要なバックアップはIBM Cloudとして取得しています。 〈ご参考〉 ・IBM クラウド・セキュリティガイドブック	適合可能	文献[03]の220スライド目にて、バックアップは自動的に日次取得されており、14世代のイメージを保存していることを確認した。 文献[03]の220スライド目にて、バックアップイメージはICOSに保管され自動的に複数のデータセンターにコピーされていることを確認した。 文献[03]の220スライド目にて、ログミラーリングによる冗長化構成（HADR機能によるローカルHAを提供）をとっており、障害時にもトランザクションをロスせずスタンバイノードへの引継を完了できることを確認した。 文献[03]の220スライド目にて、ローカルの冗長化に加え、万が一の災害時やメンテナンス時のサービス継続のために他地域にもデータベースを構成可能であることを確認した。	公開文書	文献[03]	―	―	―	利用者は、重要なプログラムのバックアップを取得し、保管管理方法を明確にする必要がある。
実42	IBM Cloud 環境では以下のポリシーに従いネットワーク設定情報が適切に管理されています。 IBM は、「クラウド・サービス」に対する変更の適用に関連するリスクの管理を目的として設計されたポリシーおよび手続きを維持します。「クラウド・サービス」（そのシステム、ネットワークおよび基盤となるコンポーネントを含みます。）に対する変更は、実装前に、登録された変更要求として文書化されます。当該変更要求には、変更の説明および〝理由、実装の詳細およびスケジュール、「クラウド・サービス」およびそのお客様に対する影響に対処するリスク・ステートメント、予期される結果、ロールバック計画ならびに権限のある担当者の文書による承認を含むものとします。 〈ご参考〉 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則	適合可能	文献[03]の222スライド目にて、プライベートネットワーク接続の提供が可能であること、Source IP Filtering（ホワイトリストの設定、特定のIPアドレスからの接続のみを許可）の提供が可能であることを確認した。 文献[01]の「4.5.1. IBM Cloud インフラストラクチャーにおける ID・アクセス管理」にて、ユーザー ID とパスワード管理は IBM ID の方式に従いますが、このユーザーID に対して、管理コンソールへのアクセス許可を IP アドレスで制限したり、二要素認証機能を実装したりすることが可能であることを確認した。 文献[01]の「4.5.1. IBM Cloud インフラストラクチャーにおける ID・アクセス管理」にて、「サポート」「デバイス」「ネットワーク」「セキュリティ」「サービス」「アカウント」からなる詳細な権限設定、およびサーバーへのアクセス権限を管理することにより、きめ細やかなアクセス制御を実施することができることを確認した。 文献[01]の「4.6.1. IBM Cloud インフラストラクチャーにおける運用管理」にて、IBM Cloud インフラストラクチャーのネットワークや IMS と呼ばれるコアシステムには、専門の運用チームが世界中の拠点から常時監視・保守を行っており、データセンターへの立ち入りを許可されていないことを確認した。 文献[01]の「4.6.1. IBM Cloud インフラストラクチャーにおける運用管理」にて、IBM Cloud インフラストラクチャーの運用チームや開発チームがIMS（情報管理システム）にログインするためにはVPN および二要素認証の両方を必ず必須としていることを確認した。 なお、IMS（情報管理システム）へのアクセスログは常に取得されており、それぞれの業務を遂行するにあたっての必要最低限のアクセス権限のみ付与されることを確認した。 文献[01]の「4.6.3. IBM Cloud プラットフォーム」にて、IBM Cloud プラットフォームではマネージド・サービスとして、専門の運用チームが世界中の拠点から常時監視を実施していることを確認し	公開文書	文献[01] 文献[03]	―	―	―	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実43	IBM Cloud 環境では以下のポリシーに従いネットワーク設定情報が適切に管理されています。 IBM は、「クラウド・サービス」に対する変更の適用に関連するリスクの管理を目的として設計されたポリシーおよび手続きを維持します。「クラウド・サービス」（そのシステム、ネットワークおよび基盤となるコンポーネントを含みます。）に対する変更は、実装前に、登録された変更要求として文書化されます。当該変更要求には、変更の説明および〝理由、実装の詳細およびスケジュール、「クラウド・サービス」およびそのお客様に対する影響に対処するリスク・ステートメント、予期される結果、ロールバック計画ならびに権限のある担当者の文書による承認を含むものとします。 〈ご参考〉 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則	適合可能	文献[01]の「4.3.2. IBM Cloud プラットフォームにおけるデータ・セキュリティ」にて、クラウド事業者としてサービス運用上必要となるデータのバックアップについてはクラウド事業者により取得され、すべて暗号化されインターネットから直接アクセスできない領域に保管されていることを確認した。	公開文書	文献[01]	－	－	－	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実44	IBM Cloud 環境では以下のポリシーに従い運用時ドキュメントが適切に管理されています。 IBM は、「クラウド・サービス」に対する変更の適用に関連するリスクの管理を目的として設計されたポリシーおよび手続きを維持します。「クラウド・サービス」（そのシステム、ネットワークおよび基盤となるコンポーネントを含みます。）に対する変更は、実装前に、登録された変更要求として文書化されます。当該変更要求には、変更の説明および〝理由、実装の詳細およびスケジュール、「クラウド・サービス」およびそのお客様に対する影響に対処するリスク・ステートメント、予期される結果、ロールバック計画ならびに権限のある担当者の文書による承認を含むものとします。 〈ご参考〉 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則	適合可能	文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 8.2.3 資産の取り扱い JIS Q 27002 の8.2.3 に定める管理策及び付随する実施の手引を適用する。 － 12.1.1 操作手順書 JIS Q 27002 の12.1.1 に定める管理策及び付随する実施の手引を適用する。 文献[01]の「4.3.2. IBM Cloud プラットフォームにおけるデータ・セキュリティ」にて、クラウド事業者としてサービス運用上必要となるデータのバックアップについてはクラウド事業者により取得され、すべて暗号化されインターネットから直接アクセスできない領域に保管されていることを確認した。 文献[07]の「3. セキュリティー・インシデント a」にて、IBMは、コンピューターのセキュリティー・インシデントの取り扱いについてのNISTガイドラインに合致する、文書化されたインシデント対応ポリシーを維持管理してこれに従い、本契約のデータ漏えいの通知に関する条件を厳守することを確認した。	公開文書	文献[01] 文献[07] 文献[09]	ISO27017 8.2.3 12.1.1	－	－	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実45	IBM Cloud 環境では以下のポリシーに従い復旧に必要なドキュメントが適切に管理されています。 IBM は、「クラウド・サービス」に対する変更の適用に関連するリスクの管理を目的として設計されたポリシーおよび手続きを維持します。「クラウド・サービス」（そのシステム、ネットワークおよび基盤となるコンポーネントを含みます。）に対する変更は、実装前に、登録された変更要求として文書化されます。当該変更要求には、変更の説明および〝理由、実装の詳細およびスケジュール、「クラウド・サービス」およびそのお客様に対する影響に対処するリスク・ステートメント、予期される結果、ロールバック計画ならびに権限のある担当者の文書による承認を含むものとします。 文書は定期的にバックアップが取得され、適切なバックアップ設備にて保管されています。 セキュリティマニュアルやSOC2において方式が準備されている 〈ご参考〉 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・Core Controls for C3 Compliance Program ・Security Manual	適合可能	文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 12.3.1 情報のバックアップ JIS Q 27002 の12.3.1 に定める管理策及び付随する実施の手引を適用する。次のクラウドサービス固有の実施の手引も適用する。 文献[07]の「6. サービスの感染性および可用性管理 d」にて、各IBM「クラウド・サービス」には、当該リスク・アセスメントで保証される範囲において、業界標準の実務に合致する事業継続性および災害復旧の計画が付帯することを確認した。 なお、当該計画は、個別に定義され、文書化され、維持され、毎年検証されることを確認できた。 文献[01]の「4.3.2. IBM Cloud プラットフォームにおけるデータ・セキュリティ」にて、クラウド事業者としてサービス運用上必要となるデータのバックアップについてはクラウド事業者により取得され、すべて暗号化されインターネットから直接アクセスできない領域に保管されていることを確認した。 文献[07]の「3. セキュリティー・インシデント a」にて、IBMは、コンピューターのセキュリティー・インシデントの取り扱いについてのNISTガイドラインに合致する、文書化されたインシデント対応ポリシーを維持管理してこれに従い、本契約のデータ漏えいの通知に関する条件を厳守することを確認した。	公開文書	文献[01] 文献[07] 文献[09]	ISO27017 12.3.1	－	－	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実46	IBMではNetwork Operations Center(NOC)とSecurity Operation Center(SOC)のチームが、IBM Cloudの環境を24/365監視し、問題の特定およびインシデント対応の責任を負います。 また、IBM Cloud インフラストラクチャーのネットワークや IMS と呼ばれるコアシステムには、専門の運用チームが世界中の拠点から常時監視・保守を行っています。 なお、お客様のアプリケーションの死活監視および各種ログの収集、提供はIBM Cloud プラットフォームの機能として有しており、その他の業務に必要な運用の設計、実装はお客様にて実施いただく必要があります。 ＜ご参考＞ ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・IBMクラウド・セキュリティガイドブック ・技術よりな人が最初に読む IBM Cloud柔らか層本	適合可能	文献[03]の246スライド目にて、Network Operations Center(NOC)とSecurity Operation Center(SOC)のチームが、IBM Cloudの環境を24/365監視し、問題の特定およびインシデント対応の責任を負うことを確認した。 文献[01]の「4.6.1. IBM Cloud インフラストラクチャーにおける運用管理」にて、IBM Cloud インフラストラクチャーのネットワークや IMS と呼ばれるコアシステムには、専門の運用チームが世界中の拠点から常時監視・保守を行っており、データセンターへの立ち入りを許可されていないことを確認した。 文献[01]の「4.6.3」にて、IBM Cloud プラットフォームではマネージド・サービスとして、専門の運用チームが世界中の拠点から常時監視を実施していることを確認した。 お客様のアプリケーションの死活監視および各種ログの収集、提供は IBM Cloud プラットフォームの機能として有しており、その他の業務に必要な運用の設計、実装はお客様にて実施いただくことを確認した。	公開文書	文献[01] 文献[03]	－	－	－	利用者がIBM Cloud上で構築する環境での監視対象、監視内容及び監視方法については、利用者が整備する必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実47	・IBM は、「クラウド・サービス」の運用において使用されるすべての情報技術資産のインベントリーを維持管理します。 ・IBMは、「クラウド・サービス」および基盤となるコンポーネントの正常性および可用性を継続的にモニターします。 ・利用者は、実装するアプリケーション実行環境について、監視に関する対応を実施する必要があります。 ＜ご参考＞ ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則	適合可能	文献[03]の246スライド目にて、Network Operations Center(NOC)とSecurity Operation Center(SOC)のチームが、IBM Cloudの環境を24/365監視し、問題の特定およびインシデント対応の責任を負うことを確認した。 文献[01]の「4.6.3」にて、IBM Cloud プラットフォームではマネージド・サービスとして、専門の運用チームが世界中の拠点から常時監視を実施していることを確認した。 お客様のアプリケーションの死活監視および各種ログの収集、提供は IBM Cloud プラットフォームの機能として有しており、その他の業務に必要な運用の設計、実装はお客様にて実施いただくことを確認した。	公開文書	文献[01] 文献[03]	－	－	－	利用者は、各種資源の能力及び使用状況の確認を行い、システムの性能強化や機能強化、組み合わせの再検討等を行う必要がある。
実48	・利用者はOS等のインストールにあたりIBM Cloudからライセンスを購入できます。 ・ハードウェア構成情報およびIBM Cloud経由で提供されるソフトウェアの構成情報はIMS機能により管理され、IBM Cloud社内の構成管理に利用されるほか、利用者向けにも開示されており、例えば製造ロットの確認を行うことも可能です。 ・利用者は、実装するアプリケーションで利用するソフトウェアの管理を実施する必要があります。 ・利用者は、仮想マシンなどのリソースの追加・構成・削除ができ、ゲストOS、ソフトウェアのコントロール、仮想アプライアンスの導入を行うことができます。その管理は利用者の責任となります。 ＜ご参考＞ ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[02]の「6. サービスの完全性および可用性管理　c」にて、IBM は、「クラウド・サービス」および基盤となるコンポーネントの正常性および可用性を継続的にモニターすることを確認した。 文献[03]の468スライド目にて、IBM Cloud IaaSのサーバに関する機器情報は全て管理システムに登録・管理していることを確認した。	公開文書	文献[02] 文献[03]	－	－	－	資産の所有者は、資産一覧の中でその資産の情報（所有者または関連する代理人、場所、セキュリティ分類など）が最新であるように保守する責任を負い、資産保護を規格に応じて分類し、保守する役割を担う。 利用者は、自身のデータの管財人としての責任を負う。
実49	IBM は、新規採用者全員について、自社の標準の必須の雇用検証要件を維持し、これに従います。また、当該要件の遵守を IBM の完全子会社にも拡大して適用します。IBM の社内プロセスおよび手続きに従って、これらの要件は定期的に見直されます。また雇用確認要件には、犯罪歴の確認、身元確認の証拠および IBM が必要とみなすその他の確認が含まれます。IBM の各法人は、現地の法律に基づいて許容され、かつ適用可能な範囲で、適宜、その採用プロセスに上記の要件を組み込む責任を負います。 また、データセンターのオペレーターはその役割に基づいてアクセス権を付与しています。 ＜ご参考＞ ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance ・Security Manual	適合可能	NDA文献[N04]にて、アクセスコントロールに関するルールが定められていることを確認した。 NDA文献[N01]の PS02.1 Perimeter Doorsにて、物理的に元々扉は施錠されており、CASにてアクセスコントロールされていることを確認した。 文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 －　9.1.1 アクセス制御方針 JIS Q 27002 の9.1.1 に定める管理策並びに付随する実施の手引及び関連情報を適用する。 文献[02]の「4. 物理的セキュリティーおよび入場管理　d」にて、IBM は、「クラウド・サービス」の物理的インフラストラクチャーを、自然発生的および人為的な環境脅威（極端な周辺温度、火災、洪水、湿度、窃盗、および破壊行為など）から保護するための予防措置を講じることを確認した。 文献[01]の「4.1.1. IBM Cloud インフラストラクチャーにおける物理セキュリティ」にて、お客様環境を容易に特定できないようにするため、サーバー内の機器はバーコードのみでID 管理しており、お客様環境を外部から特定できるような印を付けていないことを確認した。	要NDA	文献[01] 文献[02] 文献[09]	ISO27017 9.1.1	－	NDA文献[N01] NDA文献[N04]	利用者がIBM Cloudへ接続するために機器・ネットワーク等を設置する場合は、当該環境における対策は利用者にて実施する必要がある。
実50	・IBM は、「クラウド・サービス」の物理的インフラストラクチャーを、自然発生的および人為的な環境脅威（極端な周辺温度、火災、洪水、湿度、窃盗、および破壊行為など）から保護するための予防措置を講じます。 ・利用者は、実装するアプリケーションのネットワーク構成を管理する必要があります。利用者は、仮想マシンなどのリソースの追加・構成・削除ができ、ゲストOS、ソフトウェアのコントロール、仮想アプライアンスの導入を行うことができます。その管理は利用者の責任となります。 ＜ご参考＞ ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・IBMクラウド・セキュリティガイドブック ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[02]の「4. 物理的セキュリティーおよび入場管理　d」にて、IBM は、「クラウド・サービス」の物理的インフラストラクチャーを、自然発生的および人為的な環境脅威（極端な周辺温度、火災、洪水、湿度、窃盗、および破壊行為など）から保護するための予防措置を講じることを確認した。	公開文書	文献[02]	－	－	－	利用者がIBM Cloudへ接続するために機器・ネットワーク等を設置する場合は、当該環境における対策は利用者にて実施する必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実51	・IBM Cloudでは基金の可用性および完全性を継続的に維持することを確実にするために、定期的に保守を実施しています。 ・IBM Cloudでは機器の計画保守についてコンソール画面およびメールにて通知をしています。 <ご参考> ・IBMクラウド・セキュリティガイドブック ・IBM Cloud Service Description https://www-03.ibm.com/software/sla/sladb.nsf/sla/bm-6605-12 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance ・IBM Cloud	適合可能	インタビューにて、IBM Couldのポータル画面で計画保守の予定が一覧化され、常時閲覧可能であることを確認した。 インタビューにて、メーカの定める保守スペースの設置基準を配慮して機器を設置しており、保守点検の項目を定め、電源、空調、防災、防犯に係る各種設備の保守点検を実施していることを確認した。	要NDA	―	―	IBM Couldのポータル画面で計画保守の予定が一覧化され、常時閲覧可能である。 メーカの定める保守スペースの設置基準を配慮して機器を設置しており、保守点検の項目を定め、電源、空調、防災、防犯に係る各種設備の保守点検を実施している。	―	利用者がIBM Cloudへ接続するために機器・ネットワーク等を設置する場合は、当該環境における対策は利用者にて実施する必要がある。
実52	・IBM Cloudでは基金の可用性および完全性を継続的に維持することを確実にするために、定期的に保守を実施しています。 ・IBM Cloudでは機器の計画保守についてコンソール画面およびメールにて通知をしています。 <ご参考> ・IBMクラウド・セキュリティガイドブック ・IBM Cloud Service Description https://www-03.ibm.com/software/sla/sladb.nsf/sla/bm-6605-12 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance ・IBM Cloud	適合可能	インタビューにて、IBM Couldのポータル画面で計画保守の予定が一覧化され、常時閲覧可能であることを確認した。 インタビューにて、メーカの定める保守スペースの設置基準を配慮して機器を設置しており、保守点検の項目を定め、電源、空調、防災、防犯に係る各種設備の保守点検を実施していることを確認した。	要NDA	―	―	IBM Couldのポータル画面で計画保守の予定が一覧化され、常時閲覧可能である。 メーカの定める保守スペースの設置基準を配慮して機器を設置しており、保守点検の項目を定め、電源、空調、防災、防犯に係る各種設備の保守点検を実施している。	―	利用者は、利用者側環境における機器等について定期的に予防保守を行う必要がある。
実53	・IBMではクラウドサービス提供にあたり十分な管理を確実にするための責任体制および手順を備えています。 ・各データセンタに常駐する設備管理担当がコンピュータ室の温湿度を常時監視しているほか、各種設備の稼働状況を監視し、各シフトが日報を作成しています。 ・発電機等の稼働点検、各種法定点検、IBM Cloud本社設備管理担当による視察等を定期的に実施しています。 <ご参考> ・技術よりな人が最初に読む IBM Cloud柔らか層本	適合可能	文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 12.1 運用の手順及び責任 JIS Q 27002 の12.1 に定める管理目的を適用する。 文献[09]にて、SOC2の取得証明書を確認した。 なお、SOC2では、設備の管理責任者及び管理方法について記載されていることを確認した。 文献[02]の「6. サービスの完全性および可用性管理 d」にて、各「クラウド・サービス」は、事業継続性および災害復旧の要件について、文書化されたリスク管理ガイドラインに従って個別に評価されることを確認した。	公開文書	文献[02] 文献[09]	ISO27017 12.1 SOC2 P16 Environmental Controls	―	―	利用者は、システムの管理者、管理方法を定め、障害時・災害時の対応指針を明確にしたうえで、地理的な冗長性のためにアプリケーションやデータを複数のリージョンに展開する等の対策を実施する責任を負う。
実54	・項目を定め電源、空調、防災、防犯に係る各種設備の保守点検を実施しています。 ・重要設備の点検については、冗長性を考慮しながら、システムの稼働への影響回避を図っています。 <ご参考> ・技術よりな人が最初に読む IBM Cloud柔らか層本	適合可能	インタビューにて、メーカの定める保守スペースの設置基準を配慮して機器を設置しており、保守点検の項目を定め、電源、空調、防災、防犯に係る各種設備の保守点検を実施していることを確認した。	要NDA	―	―	メーカの定める保守スペースの設置基準を配慮して機器を設置しており、保守点検の項目を定め、電源、空調、防災、防犯に係る各種設備の保守点検を実施している。	―	利用者は、利用者側環境における機器等について定期的に保守点検を行う必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実55	・中央管理室にて空調や電源設備の稼働状況と負荷状況等を監視しています。 ・中央管理室では、次の設備等について限界設定および監視を行っています。 ・CVCF ・蓄電池 ・自家発電 ・給排水 ・消火設備 ・監視設備 ・通信回線 <ご参考> ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	インタビューにて、メーカの定める保守スペースの設置基準を配慮して機器を設置しており、保守点検の項目を定め、電源、空調、防災、防犯に係る各種設備の保守点検を実施していることを確認した。	要NDA	―	―	メーカの定める保守スペースの設置基準を配慮して機器を設置しており、保守点検の項目を定め、電源、空調、防災、防犯に係る各種設備の保守点検を実施している。	―	利用者は、利用者側環境における各種設備の使用状況の確認を行う必要がある。
実56	・データセンターの入退室管理 アクセスコントロールがあり、24時間監視された施設を利用しています。 生体認証セキュリティが、データセンター全体で利用されています。 監視カメラ（CCTV）による監視がされており、ログは少なくとも90日間保存されます。 ・サーバールームの特徴 デジタルセキュリティビデオによる監視がされています。 利用者側に設置される設備（オンプレミス側の管理端末・サーバー等）の管理は利用者の責任となります。 <ご参考> ・技術よりな人が最初に読む IBM Cloud柔らか層本 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・IBMクラウド・セキュリティガイドブック ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[02]の「4. 物理的セキュリティーおよび入場管理 a」にて、IBM は、「クラウド・サービス」のホストに使用される IBM 施設（データセンター）への不正な入場から保護するため、適切に物理的な入場管理（柵、カード制御の入口、監視カメラ、および有人の受付デスクなど）を維持管理していることを確認した。 文献[02]の「4. 物理的セキュリティーおよび入場管理 b」にて、データセンターおよびデータセンター内の管理エリアへのアクセスは、職務別に制限され、権限ある承認が必要になることを確認した。 文献[02]の「4. 物理的セキュリティーおよび入場管理 b」にて、管理されたデータセンター・エリアへのアクセス権限を有する従業員が離職するにあたって、IBM は、当該従業員のアクセス権限を取り消すことを確認した。 文献[02]の「4. 物理的セキュリティーおよび入場管理 c」にて、データセンター施設、またはデータセンター内の管理エリアに入場する一時的な許可を正式に付与されたいかなる個人も、当該施設に入場する際に登録され、登録時に身分証明書の提示が義務付けられ、権限ある要員が付き添うことを確認した。 文献[02]の「4. 物理的セキュリティーおよび入場管理 c」にて、搬出・搬入を含む、入場のための一時的な許可は、事前の計画および権限ある承認を必要とすることを確認した。 文献[01]の「4.1.1. IBM Cloud インフラストラクチャーにおける物理セキュリティ」にて、データセンターの建物は24 時間監視体制のもと、データセンター周辺の公道から警備員を配置していることを確認した。 文献[01]の「4.1.1. IBM Cloud インフラストラクチャーにおける物理セキュリティ」にて、建物への入館には必ず受付を通る必要があり、建物内の共通のエリアにはさらに入館チェックを通過する	公開文書	文献[01] 文献[02]	―	―	―	利用者は、利用者側環境における入退館（室）及び鍵管理を適切に行う必要がある。
実57	データセンターの入退室管理 アクセスコントロールがあり、24時間監視された施設を利用しています。 生体認証セキュリティが、データセンター全体で利用されています。 監視カメラ（CCTV）による監視がされており、ログは少なくとも90日間保存されます。 サーバールームの特徴 デジタルセキュリティビデオによる監視がされています。 利用者側に設置される設備（オンプレミス側の管理端末・サーバー等）の管理は利用者の責任となります。 <ご参考> ・技術よりな人が最初に読む IBM Cloud柔らか層本 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・IBMクラウド・セキュリティガイドブック ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[02]の「4. 物理的セキュリティーおよび入場管理 a」にて、IBM は、「クラウド・サービス」のホストに使用される IBM 施設（データセンター）への不正な入場から保護するため、適切に物理的な入場管理（柵、カード制御の入口、監視カメラ、および有人の受付デスクなど）を維持管理していることを確認した。 文献[02]の「4. 物理的セキュリティーおよび入場管理 b」にて、データセンターおよびデータセンター内の管理エリアへのアクセスは、職務別に制限され、権限ある承認が必要になることを確認した。 文献[02]の「4. 物理的セキュリティーおよび入場管理 b」にて、管理されたデータセンター・エリアへのアクセス権限を有する従業員が離職するにあたって、IBM は、当該従業員のアクセス権限を取り消すことを確認した。 文献[02]の「4. 物理的セキュリティーおよび入場管理 c」にて、データセンター施設、またはデータセンター内の管理エリアに入場する一時的な許可を正式に付与されたいかなる個人も、当該施設に入場する際に登録され、登録時に身分証明書の提示が義務付けられ、権限ある要員が付き添うことを確認した。 文献[02]の「4. 物理的セキュリティーおよび入場管理 c」にて、搬出・搬入を含む、入場のための一時的な許可は、事前の計画および権限ある承認を必要とすることを確認した。 文献[01]の「4.1.1. IBM Cloud インフラストラクチャーにおける物理セキュリティ」にて、データセンターの建物は24 時間監視体制のもと、データセンター周辺の公道から警備員を配置していることを確認した。 文献[01]の「4.1.1. IBM Cloud インフラストラクチャーにおける物理セキュリティ」にて、建物への入館には必ず受付を通る必要があり、建物内の共通のエリアにはさらに入館チェックを通過する	公開文書	文献[01] 文献[02]	―	―	―	利用者は、利用者側環境における入退館（室）及び鍵管理を適切に行う必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実58	・データセンターの入退室管理 アクセスコントロールがあり、24時間監視された施設を利用しています。 生体認証セキュリティが、データセンター全体で利用されています。 ・サーバールームの特徴 IBM Cloudの従業員とエスコートされた契約者と訪問者に厳格に制限されています。 ＜ご参考＞ ・技術よりな人が最初に読む IBM Cloud柔らか層本 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[02]の「4. 物理的セキュリティーおよび入場管理 b」にて、データセンターおよびデータセンター内の管理エリアへのアクセスは、職務別に制限され、権限ある承認が必要になることを確認した。 文献[02]の「4. 物理的セキュリティーおよび入場管理 c」にて、データセンター施設、またはデータセンター内の管理エリアに入場する一時的な許可を正式に付与されたいかなる個人も、当該施設に入場する際に登録され、登録時に身分証明書の提示が義務付けられ、権限ある要員が付き添うことを確認した。	公開文書	文献[02]	－	－	－	利用者は、利用者側環境における入退館（室）及び鍵管理を適切に行う必要がある。 また、事前に入館を許可された者であっても入室に際しては再度資格確認を行う必要がある。
実59	・データセンターの入退室管理 アクセスコントロールがあり、24時間監視された施設を利用しています。 生体認証セキュリティが、データセンター全体で利用されています。 監視カメラ（CCTV）による監視がされており、ログは少なくとも90日間保存されます。 ・サーバールームの特徴 デジタルセキュリティビデオによる監視がされています。 IBM Cloudの従業員とエスコートされた契約者と訪問者に厳格に制限されています。 入室後の作業については手順書が作成され、作業者は作業手順書を適用し作業を実施しています。 ＜ご参考＞ ・技術よりな人が最初に読む IBM Cloud柔らか層本 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・IBMクラウド・セキュリティガイドブック ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[03]の238スライド目にて、サーバールームは24時間/365日、スタッフが常駐していることを確認した。 文献[03]の238スライド目にて、デジタルセキュリティビデオによる監視がされていることを確認した。 文献[03]の238スライド目にて、IBM Cloudの従業員とエスコートされた契約者と訪問者に、厳格にデータセンターの入退室が制限されていることを確認した。 文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 11.1.5 セキュリティを保つべき領域での作業 JIS Q 27002 の11.1.5 に定める管理策及び付随する実施の手引を適用する。	公開文書	文献[03] 文献[09]	ISO27017 11.1.5	－	－	利用者は、入室後における入室者の作業を適切に管理する必要がある。
実60	IBMでは機器の管理内容を明確化し、以下のような監視を行っています。 IBM Cloud インフラストラクチャーのネットワークや IMS（情報管理システム）と呼ばれるコアシステムには、専門の運用チームが世界中の拠点から常時監視・保守を行っています。 ・データセンターの入退室管理 アクセスコントロールがあり、24時間監視された施設を利用しています。 監視カメラ（CCTV）による監視がされており、ログは少なくとも90日間保存されます。 ・サーバールームの特徴 24時間/365日、スタッフが常駐しています。 デジタルセキュリティビデオによる監視がされています。 ＜ご参考＞ ・技術よりな人が最初に読む IBM Cloud柔らか層本 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 12.1 運用の手順及び責任 JIS Q 27002 の12.1 に定める管理目的を適用する。 － 13.1 ネットワークセキュリティ管理 JIS Q 27002 の13.1 に定める管理目的を適用する。 － 9.1.1 アクセス制御方針 JIS Q 27002 の9.1.1 に定める管理策並びに付随する実施の手引及び関連情報を適用する。 文献[01]の「4.6.1. IBM Cloud インフラストラクチャーにおける運用管理」にて、IBM Cloud インフラストラクチャーのネットワークや IMS（情報管理システム）と呼ばれるコアシステムには、専門の運用チームが世界中の拠点から常時監視・保守を行っており、データセンターへの立ち入りを許可されていないことを確認した。	公開文書	文献[01] 文献[09]	ISO27017 9.1.1 12.1 13.1	－	－	利用者は、利用者側環境における各種設備の監視体制を整備する必要がある。
実61	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	利用者は、顧客が操作できる権限を明確にする必要がある。
実62	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	利用者は、操作権限を付与するオペレータカード（オペレータキー、IDを含む）の管理者を定めて管理する必要がある。
実63	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	利用者は、顧客の操作内容を記録し、検証できる体制を整備する必要がある。
実64	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	利用者は、顧客からの届出の受付体制の整備、事故口座の管理を行う必要がある。
実65	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	利用者は、データの入力手続き、承認等の手順を策定する必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実66	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	利用者は、出力情報の作成、授受、保管、管理及び廃棄について、不正防止対策及び機密保護対策を講じる必要がある。
実67	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	利用者は、未使用重要帳票の在庫管理及び廃棄の方法を定める必要がある。
実68	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	利用者は、重要な印字済帳票の授受及び廃棄の方法を定める必要がある。
実69	IBM Cloudでは「IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則」に記載されている通り、顧客データの保護について規定され管理・保護されています。 <参考> ・ IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[01]の「3.2 データ管理」にて、クラウド上に置くデータの重要性に応じて、暗号化の必要性の有無、配置場所、アクセス管理、バックアップデータの取り扱い方法等に対しても、利用者自身で対策を講じる必要があることを確認した。 文献[05]の「4.1」にて、IBM は、お客様より許可を得た場合または法律により要求される場合を除き、いかなる第三者にも「お客様個人データ」を開示しないことを確認した。 文献[05]の「4.1」にて、政府または「監督機関」が「お客様個人データ」へのアクセスを要求した場合、IBM は開示前にお客様に通知することを確認した。ただし、かかる通知が法令により禁じられている場合はこの限りではない。 文献[05]の「4.2」にて、IBM は、「お客様個人データ」を「処理」する権限が与えられたすべての従業員に対し、機密保持義務を確約させ、かつ、お客様の指示に基づく場合または適用法により要求される場合を除き、他の目的のために当該「お客様個人データ」を「処理」しないことを求めることを確認した。 文献[01]の「3.2 データ管理」にて、どのサービスモデルを利用する際においても、データに関しては最終的には利用者の責任で管理する必要があることを確認した。 文献[01]の「3.2 データ管理」にて、データの重要性に応じて、どういう手段と経路を使ってどこに配置するべきかを判断し、法令遵守やコンプライアンスの観点から適切な物理的所在を考慮するのは利用者の責任になることを確認した。	公開文書	文献[01] 文献[05]	－	－	－	利用者は、顧客データの管理・取り扱い方法を定める必要がある。特に機微情報を取り扱う場合は、必要な措置を行う必要がある。
実70	IBM Cloudでは以下のポリシーに従い手順が決められています。 利用者およびIBM Cloud担当者への通知はカスタマーポータルにて行われます。 各「クラウド・サービス」は、事業継続性および災害復旧の要件について、文書化されたリスク管理ガイドラインに従って個別に評価されます。各 IBM「クラウド・サービス」には、当該リスク・アセスメントで保証される範囲において、業界標準の実務に合致する事業継続性および災害復旧の計画が付帯します。当該計画は、個別に定義され、文書化され、維持され、毎年検証されます。「クラウド・サービス」のリカバリー・ポイントおよびリカバリー時間の達成目標が提供される場合、「クラウド・サービス」のアーキテクチャーおよび使用目的を考慮して設定され、関連の個別契約書に記載されます。「クラウド・サービス」のバックアップ・ファイルが保存されたメディアなど、オフサイトで保管される物理媒体がある場合は、転送前に暗号化されます。 <ご参考> ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[07]の「6. サービスの感染性および可用性管理 d」にて、各「クラウド・サービス」は、事業継続性および災害復旧の要件について、文書化されたリスク管理ガイドラインに従って個別に評価されることを確認した。 文献[06]の「2.1安全で生産的な作業環境の維持」にて、携帯電話番号を含む正確な緊急連絡先情報をIBM社員セーフ・ツールの中に登録していることを確認した。 文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 16.1.1 責任及び手順 JIS Q 27002 の16.1.1 に定める管理策並びに付随する実施の手引及び関連情報を適用する。	公開文書	文献[06] 文献[07] 文献[09]	ISO27017 16.1.1	－	－	利用者は、システムの管理者、管理方法を定め、障害時・災害時の対応指針を明確にしたうえで、地理的な冗長性のためにアプリケーションやデータを複数のリージョンに展開する等の対策を実施する責任を負う。
実71	IBM Cloudでは以下のポリシーに従いサービス復旧・継続に必要な情報が遠隔地保管されています。 各「クラウド・サービス」は、事業継続性および災害復旧の要件について、文書化されたリスク管理ガイドラインに従って個別に評価されます。各 IBM「クラウド・サービス」には、当該リスク・アセスメントで保証される範囲において、業界標準の実務に合致する事業継続性および災害復旧の計画が付帯します。当該計画は、個別に定義され、文書化され、維持され、毎年検証されます。「クラウド・サービス」のリカバリー・ポイントおよびリカバリー時間の達成目標が提供される場合、「クラウド・サービス」のアーキテクチャーおよび使用目的を考慮して設定され、関連の個別契約書に記載されます。「クラウド・サービス」のバックアップ・ファイルが保存されたメディアなど、オフサイトで保管される物理媒体がある場合は、転送前に暗号化されます。 <ご参考> ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[07]の「6. サービスの感染性および可用性管理 d」にて、各「クラウド・サービス」は、事業継続性および災害復旧の要件について、文書化されたリスク管理ガイドラインに従って個別に評価されることを確認した。 文献[07]の「6. サービスの感染性および可用性管理 d」にて、各IBM「クラウド・サービス」にて、当該リスク・アセスメントで保証される範囲において、業界標準の実務に合致する事業継続性および災害復旧の計画が付帯することを確認した。当該計画は、個別に定義され、文書化され、維持され、毎年検証されることを確認できた。 文献[07]の「6. サービスの感染性および可用性管理 d」にて、「クラウド・サービス」のリカバリー・ポイントおよびリカバリー時間の達成目標が提供される場合、「クラウド・サービス」のアーキテクチャーおよび使用目的を考慮して設定され、関連のTD（取引文書）に記載されることを確認した。	公開文書	文献[07]	－	－	－	利用者がIBM Cloud上で構築した環境については、障害時・災害時に利用者自身が実施すべきコンピュータシステムの復旧手順を明確にする必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実72	広域障害の場合、影響の範囲や根本原因分析、再発防止策などが記載されたReport for Outage（RFO）が提供されます。 個別に発生した障害ではRFOは提供されません。ご注意ください。 〈ご参考〉 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[07]の「6. サービスの感染性および可用性管理 d」にて、各「クラウド・サービス」は、事業継続性および災害復旧の要件について、文書化されたリスク管理ガイドラインに従って個別に評価されることを確認した。 文献[07]の「6. サービスの感染性および可用性管理 d」にて、各IBM「クラウド・サービス」にて、当該リスク・アセスメントで保証される範囲において、業界標準の実務に合致する事業継続性および災害復旧の計画が付帯することを確認した。当該計画は、個別に定義され、文書化され、維持され、毎年検証されることを確認できた。 文献[07]の「6. サービスの感染性および可用性管理 d」にて、「クラウド・サービス」のリカバリー・ポイントおよびリカバリー時間の達成目標が提供される場合、「クラウド・サービス」のアーキテクチャーおよび使用目的を考慮して設定され、関連のTD（取引文書）に記載されることを確認した。 文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 16.1.6 情報セキュリティインシデントからの学習 JIS Q 27002 の16.1.6 に定める管理策並びに付随する実施の手引及び関連情報を適用する。	公開文書	文献[07] 文献[09]	ISO27017 16.1.6	－	－	利用者は、IBM Cloud上で構築した環境について障害の原因を調査する手法を講じておく必要がある。
実73	IBM Cloud サービスについては以下のポリシーによりコンティンジェンシープランが策定されています。 各「クラウド・サービス」は、事業継続性および災害復旧の要件について、文書化されたリスク管理ガイドラインに従って個別に評価されます。各 IBM「クラウド・サービス」には、当該リスク・アセスメントで保証される範囲において、業界標準の実務に合致する事業継続性および災害復旧の計画が付帯します。 なお、利用者は実装するアプリケーションに関するコンティンジェンシープランを定める必要があります。 〈ご参考〉 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[07]の「6. サービスの感染性および可用性管理 d」にて、各「クラウド・サービス」は、事業継続性および災害復旧の要件について、文書化されたリスク管理ガイドラインに従って個別に評価されることを確認した。 文献[07]の「6. サービスの感染性および可用性管理 d」にて、各IBM「クラウド・サービス」にて、当該リスク・アセスメントで保証される範囲において、業界標準の実務に合致する事業継続性および災害復旧の計画が付帯することを確認した。当該計画は、個別に定義され、文書化され、維持され、毎年検証されることを確認できた。 文献[07]の「6. サービスの感染性および可用性管理 d」にて、「クラウド・サービス」のリカバリー・ポイントおよびリカバリー時間の達成目標が提供される場合、「クラウド・サービス」のアーキテクチャーおよび使用目的を考慮して設定され、関連のTD（取引文書）に記載されることを確認した。	公開文書	文献[07]	－	－	－	利用者は、システムの管理者、管理方法を定め、障害時・災害時の対応指針を明確にしたうえで、地理的な冗長性のためにアプリケーションやデータを複数のリージョンに展開する等の対策を実施する責任を負う必要がある。
実74	IBM Cloud サービスについては以下のポリシーによりバックアップサイトを準備しています。 各「クラウド・サービス」は、事業継続性および災害復旧の要件について、文書化されたリスク管理ガイドラインに従って個別に評価されます。各 IBM「クラウド・サービス」には、当該リスク・アセスメントで保証される範囲において、業界標準の実務に合致する事業継続性および災害復旧の計画が付帯します。 なお、利用者は、実装する仮想マシンやアプリケーションについて、データバックアップサイト対応などのフォールトトレランス対策を実施する必要があります。 〈ご参考〉 ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	インタビューにて、IBM Cloudでは世界60箇所以上のデータセンターでサービスを提供しており、相互でバックアップとしての役割を担っていることを確認した。 文献[03]の473スライド目にて、共用VPNサービスのサーバーにつながらないとき、世界中のIBM CloudのデータセンターやPoPに接続することを確認した。 文献[03]の473スライド目にて、IBM Cloudコンソールは、最寄りのリージョンで管理されているコンソールにつながるようになっていることを確認した。 文献[03]の473スライド目にて、IBM Cloud側に何らかの問題があり、最寄りのリージョンへ接続できなかったり、自動的に転送されない場合の代替接続先があることを確認した。	要NDA	文献[03]	－	IBM Cloudでは世界60箇所以上のデータセンターでサービスを提供しており、相互でバックアップとしての役割を担っている。	－	仮想マシンを冗長化する場合は、IBM Cloudの冗長構成機能を用いて利用者が実施する必要がある。 本番サイトと異なる地域にバックアップサイト向けの仮想マシンを設ける場合は、利用者が適切な地理的な場所に仮想マシンを作成する必要がある。 仮想マシンの状態やデータのバックアップの作成は、IBM Cloudのレプリケーション機能を用いて利用者が実施する必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実75	IBM Cloud サービスについてはシステム開発・変更について規定しているISO27001規格に準拠しています。 また、利用者は、実装するアプリケーション利用にあたり、ソフトウェア品質確保に関する対応を実施する必要があります。 〈ご参考〉 ISO 27001 IBM Cloud Docs	適合可能	文献[09]にて、ISO27001の取得証明書を確認した。 ISO27001の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － A.14.2.2 システムの変更管理手順 開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理しなければならない。 文献[09]にて、SOC2の取得証明書を確認した。 なお、SOC2では、システム開発・変更における内容の正当性について記載されていることを確認した。 文献[02]の「6. サービスの完全性および可用性管理　b」にて、IBM は、「クラウド・サービス」に対する変更の適用に関連するリスクの管理を目的として設計されたポリシーおよび手続きを維持することを確認した。 文献[02]の「6. サービスの完全性および可用性管理　b」にて、「クラウド・サービス」（そのシステム、ネットワークおよび基盤となるコンポーネントを含みます。）に対する変更は、実装前に、変更要請として文書化した上で登録されることを確認した。 なお、当該変更要請には、変更の説明および理由、実装の詳細およびスケジュール、「クラウド・サービス」およびそのお客様に対する影響に対処するリスク・ステートメント、予期される結果、ロールバック計画、ならびに権限のある担当者の文書による承認を含むものとしていることを確認した。	公開文書	文献[02] 文献[09]	ISO27001 A.14.2.2 SOC2 P24　Change Management P25　Changes to IMS and IMS Infrastructure Devices	－	－	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実76	IBM Cloud サービスについてはテスト環境について規定しているISO27001規格に準拠しています。 また、利用者は、実装するアプリケーション利用にあたり、ソフトウェア品質確保に関する対応を実施する必要があります。 〈ご参考〉 ISO 27001 IBM Cloud Docs	適合可能	文献[09]にて、ISO27001の取得証明書を確認した。 ISO27001の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － A.12.1.4 開発環境、試験環境及び運用環境の分離 開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために、分離しなければならない。	公開文書	文献[09]	ISO27001 A.12.1.4	－	－	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実77	IBM Cloud サービスについては本番移行について規定しているISO27001規格に準拠しています。 また、利用者は、実装するアプリケーション利用にあたり、ソフトウェア品質確保に関する対応を実施する必要があります。 〈ご参考〉 ISO 27001 IBM Cloud Docs	適合可能	文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 12.1.4 開発環境，試験環境及び運用環境の分離 JIS Q 27002 の12.1.4 に定める管理策並びに付随する実施の手引及び関連情報を適用する。	公開文書	文献[09]	ISO27017 12.1.4	－	－	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実78	IBM Cloud サービスの開発ライフサイクルにおけるシステムの変更について、初期設計段階からその後の全ての保守業務に至るまで，システム，アプリケーション及び製品の完全性を確実にするため，正式な変更管理手順を文書化しています。 〈ご参考〉 ISO 27002(ISO 27017) IBM Cloud Docs Core Controls for C3 Compliance Program	適合可能	文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 14.2.2 システムの変更管理手順 JIS Q 27002 の14.2.2 に定める管理策並びに付随する実施の手引及び関連情報を適用する。	公開文書	文献[09]	ISO27017 14.2.2	－	－	利用者は、ドキュメントの作成手順を定め、適切に保管管理する必要がある。
実79	IBM Cloud サービスについてはシステム開発・変更について規定しているISO27001規格に準拠しています。 また、利用者は、実装するアプリケーション利用にあたり、ソフトウェア品質確保に関する対応を実施する必要があります。 〈ご参考〉 ISO 27001 IBM Cloud Docs	適合可能	文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 12.1.4 開発環境，試験環境及び運用環境の分離 JIS Q 27002 の12.1.4 に定める管理策並びに付随する実施の手引及び関連情報を適用する。	公開文書	文献[09]	ISO27017 12.1.4	－	－	利用者は、ドキュメントの作成手順を定め、適切に保管管理する必要がある。
実80	IBM Cloudではガイドラインにしたがって実施しています。 また、利用者は、実装するアプリケーション利用にあたり、ソフトウェア品質確保に関する対応を実施する必要があります。 アプリケーション開発は顧客により管理されており、対象外としました。 〈ご参考〉 Core Controls for C3 Compliance Program	対象外	IBM Cloudではパッケージを購入、使用がないことを確認できたため、対象外とする。	－	－	－	－	－	利用者は、IBM Cloudサービスの導入にあたり、その有効性、信頼性、生産性などを評価する体制を整備する必要がある。
実81	IBM Cloudではガイドラインにしたがって実施しています。 また、利用者は、実装するアプリケーション利用にあたり、ソフトウェア品質確保に関する対応を実施する必要があります。 アプリケーション開発は顧客により管理されており、対象外としました。 〈ご参考〉 Core Controls for C3 Compliance Program	対象外	IBM Cloudではパッケージを購入、使用がないことを確認できたため、対象外とする。	－	－	－	－	－	利用者は、IBM Cloudサービス導入後の運用にあたり、運用・管理体制を明確にする必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実82	IBMクラウドサービスでのデータの廃棄について以下のように定義されています。 契約の解約または期間満了後、IBM は、適用法でその他の方法による処理が要求される場合を除き、該当するDPA 別表の規定に従い、自己の保有する「お客様個人データ」を削除または返却します また、利用者は、実装するアプリケーションに関する廃棄について、関連部署との調整・連絡や運用終結の確認などの手順を明確にする必要があります。 <ご参考> ・データ処理補足契約書 ・クラウド・サービス契約書 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[01]の「4.3.1. IBM Cloud インフラストラクチャーにおけるデータ・セキュリティ」にて、物理サーバーの解約時にUS 国防省によって認可されたドライブ消去ソフトウェア（Defense (DoD) 5220.22-m standards）を使うことによって、ローカルディスクから削除されることを確認した。 文献[01]の「4.3.1. IBM Cloud インフラストラクチャーにおけるデータ・セキュリティ」にて、削除に失敗したディスクは完全に修復不可能な形で物理的に破壊されることを確認した。 文献[08]の「2.コンテンツおよびデータ保護 e.」にて、IBM は、「クラウド・サービス」の満了時もしくは解約時またはそれ以前にお客様から要求があった場合には、IBM のコンピューティング資源から「コンテンツ」を削除することを確認した。	公開文書	文献[01] 文献[08]	－	－	－	利用者は、システムの廃棄計画・廃棄手順を明確にし、廃棄時に機器等から情報漏洩が生じないように防止策を講ずる必要がある。
実83	IBMクラウドサービスでのデータの廃棄について以下のように定義されています。 契約の解約または期間満了後、IBM は、適用法でその他の方法による処理が要求される場合を除き、該当するDPA 別表の規定に従い、自己の保有する「お客様個人データ」を削除または返却します また、利用者は、実装するアプリケーションに関する廃棄について、関連部署との調整・連絡や運用終結の確認などの手順を明確にする必要があります。 <ご参考> ・データ処理補足契約書 ・クラウド・サービス契約書 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[01]の「4.3.1. IBM Cloud インフラストラクチャーにおけるデータ・セキュリティ」にて、削除に失敗したディスクは完全に修復不可能な形で物理的に破壊されることを確認した。 文献[01]の「4.3.1. IBM Cloud インフラストラクチャーにおけるデータ・セキュリティ」にて、物理サーバーの解約時にUS 国防省によって認可されたドライブ消去ソフトウェア（Defense (DoD) 5220.22-m standards）を使うことによって、ローカルディスクから削除されまることを確認した。 文献[01]の「4.3.1. IBM Cloud インフラストラクチャーにおけるデータ・セキュリティ」にて、削除に失敗したディスクは完全に修復不可能な形で物理的に破壊されることを確認した。	公開文書	文献[01]	－	－	－	利用者は、システムの廃棄計画・廃棄手順を明確にし、廃棄時に機器等から情報漏洩が生じないように防止策を講ずる必要がある。
実84	IBM Cloud サービスについては以下のポリシーにより予備機を準備しています。 各「クラウド・サーヒ゛ス」は、事業継続性および災害復旧の要件について、文書化されたリスク管理ガイドラインに従って個別に評価されます。各 IBM「クラウド・サービス」には、当該リスク・アセスメントで保証される範囲において、業界標準の実務に合致する事業継続性および災害復旧の計画が付帯します。 <ご参考> ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[03]の23スライド目にて、部品の障害時には、障害箇所を特定後、2時間以内に交換することを確認した。 文献[03]の66スライド目にて、Power Systems Virtual Serversではハードウェア障害時には別のホスト上で再始動するRemote Restart機能を採用していることを確認した。 文献[03]の76スライド目にて、ホストサーバーの物理障害時には、仮想サーバーが他のホストサーバーで起動されるため、可用性を維持できることを確認した。	公開文書	文献[03]	－	－	－	利用者は、IBM Cloudを利用するための重要な装置には予備を設ける必要がある。
実85	IBM Cloud サービスについては以下のポリシーにより予備機を準備しています。 各「クラウド・サーヒ゛ス」は、事業継続性および災害復旧の要件について、文書化されたリスク管理ガイドラインに従って個別に評価されます。各 IBM「クラウド・サービス」には、当該リスク・アセスメントで保証される範囲において、業界標準の実務に合致する事業継続性および災害復旧の計画が付帯します。 <ご参考> ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[03]の23スライド目にて、部品の障害時には、障害箇所を特定後、2時間以内に交換することを確認した。	公開文書	文献[03]	－	－	－	仮想マシンの状態確認やデータのバックアップの作成は、IBM Cloudの各種機能を用いて利用者が実施する必要がある。
実86	IBM Cloud サービスについては以下のポリシーにより予備機を準備しています。 各「クラウド・サーヒ゛ス」は、事業継続性および災害復旧の要件について、文書化されたリスク管理ガイドラインに従って個別に評価されます。各 IBM「クラウド・サービス」には、当該リスク・アセスメントで保証される範囲において、業界標準の実務に合致する事業継続性および災害復旧の計画が付帯します。 <ご参考> ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[03]の66スライド目にて、Power Systems Virtual Serversではハードウェア障害時には別のホスト上で再始動するRemote Restart機能を採用していることを確認した。 文献[03]の76スライド目にて、ホストサーバーの物理障害時には、仮想サーバーが他のホストサーバーで起動されるため、可用性を維持できることを確認した。 文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 17.2 冗長性 JIS Q 27002 の17.2 に定める管理目的を適用する。	公開文書	文献[03] 文献[09]	ISO27017 17.2	－	－	利用者は、IBM Cloudを利用するための重要な装置には予備を設ける必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実87	IBM Cloud サービスについては以下のポリシーにより予備機を準備しています。 各「クラウド・サーヒ゛ス」は、事業継続性および災害復旧の要件について、文書化されたリスク管理ガイドラインに従って個別に評価されます。各 IBM「クラウド・サービス」には、当該リスク・アセスメントで保証される範囲において、業界標準の実務に合致する事業継続性および災害復旧の計画が付帯します。 <ご参考> ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[03]の127スライド目にて、IBM Cloudのデータセンターには、複数のインターネットキャリアが10Gbps x Nのインターネット回線を引き込んでいることを確認した。	公開文書	文献[03]	－	－	－	利用者は、IBM Cloudを利用するための重要な装置には予備を設ける必要がある。
実88	IBM Cloudではネットワーク経由でリモートによるオペレーションを実施しており、個別の端末に依存しないため対象外とします。 クラウド・サービスを利用する利用者の端末については利用者側で必要に応じて対応するため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	利用者は、IBM Cloudを利用するための端末系装置には予備または代替機能を設ける必要がある。
実89	IBM Cloud サービスについてはシステム開発・変更について規定しているISO27001規格に準拠しています。 また、利用者が作成するプログラムについては利用者側での対応が必要になります。 <ご参考> ISO 27001 IBM Cloud Docs	適合可能	文献[09]にて、ISO27001の取得証明書を確認した。 ISO27001の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － A.14.2.5 セキュリティに配慮したシステム構築の原則 セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの実装に対して適用しなければならない。	公開文書	文献[09]	ISO27001 A14.2.5	－	－	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実90	IBM Cloud サービスについてはシステム開発・変更について規定しているISO27001規格に準拠しています。 また、利用者は、実装するアプリケーション利用にあたり、ソフトウェア品質確保に関する対応を実施する必要があります。 <ご参考> ISO 27001 IBM Cloud Docs	適合可能	文献[09]にて、ISO27001の取得証明書を確認した。 ISO27001の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － A.14.2.5 セキュリティに配慮したシステム構築の原則 セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの実装に対して適用しなければならない。	公開文書	文献[09]	ISO27001 A14.2.5	－	－	利用者がIBM Cloud上で構築するミドルウェアやアプリケーションソフトウェアの信頼性については、利用者が対策する必要がある。
実91	IBM Cloud サービスについてはシステム開発・変更について規定しているISO27001規格に準拠しています。 また、利用者は、実装するアプリケーション利用にあたり、ソフトウェア品質確保に関する対応を実施する必要があります。 <ご参考> ISO 27001 IBM Cloud Docs	適合可能	文献[09]にて、ISO27001の取得証明書を確認した。 ISO27001の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － A.14.2.5 セキュリティに配慮したシステム構築の原則 セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの実装に対して適用しなければならない。	公開文書	文献[09]	ISO27001 A14.2.5	－	－	利用者がIBM Cloud上で構築するミドルウェアやアプリケーションソフトウェアの信頼性については、利用者が対策する必要がある。
実92	IBM Cloud サービスについてはシステム開発・変更について規定しているISO27001規格に準拠しています。 また、利用者は、実装するアプリケーション利用にあたり、ソフトウェア品質確保に関する対応を実施する必要があります。 <ご参考> ISO 27001 IBM Cloud Docs	適合可能	文献[09]にて、ISO27001の取得証明書を確認した。 ISO27001の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － A.14.2.1 セキュリティに配慮した開発のための方針 ソフトウェア及びシステムの開発のための規則は，組織内において確立し，開発に対して適用しなければならない。 － A.14.2.9 システムの受け入れ試験 新しい情報システム，及びその改訂版・更新版のために，受け入れ試験のプログラム及び関連する基準を確立しなければならない。	公開文書	文献[09]	ISO27001 A.14.2.1 A.14.2.9	－	－	利用者がIBM Cloud上で構築するミドルウェアやアプリケーションソフトウェアの信頼性については、利用者が対策する必要がある。
実93	IBM Cloudでは、各OS用にアップデートサーバーが設置され、最新のモジュールやウィルス定義ファイルを参照できます。 <ご参考> ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[03]の270スライド目にて、IBM Cloudでは、各OS用にアップデートサーバーが設置され、最新のモジュールやウィルス定義ファイルを参照できることを確認した。 文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 － 12.2.1 マルウェアに対する管理策 JIS Q 27002 の12.2.1 に定める管理策並びに付随する実施の手引及び関連情報を適用する。 － 14.2.2 システムの変更管理手順 JIS Q 27002 の14.2.2 に定める管理策並びに付随する実施の手引及び関連情報を適用する。	公開文書	文献[03] 文献[09]	ISO27017 12.2.1 14.2.2	－	－	利用者がIBM Cloud上で構築するミドルウェアやアプリケーションソフトウェアの信頼性については、利用者が対策する必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実94	IBM Cloudではガイドラインにしたがって実施しています。 また、利用者は、実装するアプリケーション利用にあたり、ソフトウェア品質確保に関する対応を実施する必要があります。 アプリケーション開発は利用者により管理されており、対象外とします。 〈ご参考〉 Core Controls for C3 Compliance Program	対象外	IBM Cloudではパッケージを購入、使用がないことを確認できたため、対象外とする。	－	－	－	－	－	利用者がIBM Cloud上で構築するミドルウェアやアプリケーションソフトウェアの信頼性については、利用者が対策する必要がある。
実95	・利用者の申し込みに応じたサーバ構築は手順化および自動化を推進し、速やかな処理と誤操作防止を図っています。 ・利用者は、仮想マシンなどの リソースの追加・構成・削除ができ、ゲストOS、ソフトウェア及びアプリケーションのコントロールを行うことができます。 〈ご参考〉 ・技術よりな人が最初に読む:IBMCloud柔らか層本	適合可能	文献[03]の228スライド目にて、運用は人手を介さないよう極力自動化していることを確認した。 文献[07]の「6. サービスの完全性および可用性管理　b」にて、IBM は、「クラウド・サービス」に対する変更の適用に関連するリスクの管理を目的として設計されたポリシーおよび手続きを維持することを確認した。 文献[07]の「6. サービスの完全性および可用性管理　b」にて、「クラウド・サービス」(そのシステム、ネットワークおよび基盤となるコンポーネントを含みます。) に対する変更は、実装前に、登録された変更要求として文書化されることを確認した。 文献[07]の「6. サービスの完全性および可用性管理　b」にて、当該変更要求には、変更の説明および理由、実装の詳細およびスケジュール、「クラウド・サービス」およびそのお客様に対する影響に対処するリスク・ステートメント、予期される結果、ロールバック計画、ならびに権限のある担当者の文書による承認を含むものであることを確認した。 文献[07]の「6. サービスの完全性および可用性管理」にて、セキュリティー・アドバイザリー・パッチの実装は、IBM の変更管理ポリシーに従って行われることを確認した。	公開文書	文献[03] 文献[07]	－	－	－	利用者がIBM Cloud上で構築するミドルウェアやアプリケーションソフトウェアの信頼性については、利用者が対策する必要がある。
実96	新しいシステムの導入及び既存システムに対する重要な変更は，文書化，仕様化，試験，品質管理及び管理された実装からなる正式な手続に従っています。 〈ご参考〉 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance ・Core Controls for C3 Compliance Program	適合可能	文献[09]にて、SOC2の取得証明書を確認した。 なお、SOC2では、機能の変更、追加作業時の品質向上対策について記載されていることを確認した。	公開文書	文献[09]	SOC2 P24　Change Management P25　Changes to IMS and IMS Infrastructure Devices	－	－	利用者がIBM Cloud上で構築するミドルウェアやアプリケーションソフトウェアの信頼性については、利用者が対策する必要がある。
実97	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	利用者がIBM Cloud上で構築するアプリケーションやサービスで矛盾発生を防止するためには、利用者が必要な対策を行う必要がある。
実98	金融機関内部の統制のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	利用者がIBM Cloud上で構築するアプリケーションやサービスで扱うファイル間の不整合を発見するためには、それらのアプリケーションやサービスで突合機能を設ける必要がある。
実99	・利用者の申し込みに応じたサーバ構築は自動化し、速やかな処理と誤操作防止を図っています。 ・利用者の問合せに応じたチケット発行とIBM Cloud要員への通知は自動化され、進捗管理も自動化を進め、対応漏れや遅延の回避を図っています。 ・利用者は、実装するアプリケーションが稼働する仮想マシン等のオペレーションの自動化・簡略化について対応する必要があります。 〈ご参考〉 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[03]の228スライド目にて、運用は人手を介さないよう極力自動化していることを確認した。 文献[03]の41スライド目にて、サーバーのCPU使用率やネットワーク使用状況に応じ、サーバー台数を動的に増減するオート・スケール機能を有しており、リソース不足を予測して自動的にプロビジョニングされることが確認できた。	公開文書	文献[03]	－	－	－	利用者がIBM Cloud上で構築するアプリケーションやサービスの運用における信頼性については、利用者が対策する必要がある。
実100	・利用者の申し込みに応じたサーバ構築は自動化し、速やかな処理と誤操作防止を図っています。 ・定型的なネットワーク構成変更はスクリプト機能を活用し、変更自体を自動化しています。 ・利用者は、実装するアプリケーションが稼働する仮想マシン等のオペレーションの自動化・簡略化について対応する必要があります。 ＜ご参考＞ ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[09]にて、ISO27017の取得証明書を確認した。 ISO27017の以下の要件に準拠しているため、当FISC要件に準拠していると推測される。 －　CLD.12.1.5 運用の手順及び責任 クラウドコンピューティングには，迅速な提供及び管理並びにオンデマンドセルフサービスという利点がある。これらの操作は，多くの場合，クラウドサービスカスタマ及びクラウドサービスプロバイダの実務管理者が行う。これらの重要な操作への人間の介入は重大な情報セキュリティインシデントを引き起こす可能性があるため，操作を保護するための仕組みの導入を検討することが望ましく，必要に応じてこれを定義し実施することが望ましい。 文献[03]の228スライド目にて、運用は人手を介さないよう極力自動化していることを確認した。 文献[01]の「4.1.1. IBM Cloud インフラストラクチャーにおける物理セキュリティ」にて、お客様ごとのネットワーク構成やネットワーク設定などの作業は全て内部システムにより自動化されており、属人的な作業を可能な限り廃していることを確認した。	公開文書	文献[01] 文献[03] 文献[09]	ISO27017 CLD.12.1.5	－	－	利用者がIBM Cloud上で構築するアプリケーションやサービスの運用における信頼性については、利用者が対策する必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実101	・システムの負荷状態を監視し、IMS機能により利用者向け開示を行っています。 ・各種資源で一時的に不足状態が発生した場合には、プロビジョニング時に不足資源が選択できなくなる機能を活用し、制御しています。 ・利用者は、実装するアプリケーションの監視と対応策に関する対応を実施する必要があります。 ＜ご参考＞ ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[02]にて、IBMは、「クラウド・サービス」および基盤となるコンポーネントの正常性および可用性を継続的にモニターすることが確認できた。 文献[03]の190スライド目にて、複数のアプリケーションを稼働させるための管理し、個々のアプリケーション・インスタンスの配置や、実行状況の監視や状況に応じた管理を実行していることを確認した。	公開文書	文献[02] 文献[03]	–	–	–	利用者がIBM Cloud上で構築するアプリケーションやサービスの監視制御については、利用者が行うがある。
実102	・各種ツールを導入して稼動状況の監視が行われています。 ・利用者は、実装するアプリケーションに関して、システムの重要性に応じた監視に関する対応を実施する必要があります。 ＜ご参考＞ ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[02]にて、IBMは、「クラウド・サービス」および基盤となるコンポーネントの正常性および可用性を継続的にモニターすることが確認できた。 文献[03]の190スライド目にて、複数のアプリケーションを稼働させるための管理し、個々のアプリケーション・インスタンスの配置や、実行状況の監視や状況に応じた管理を実行していることを確認した。	公開文書	文献[02] 文献[03]	–	–	–	利用者がIBM Cloud上で構築するアプリケーションやサービスの障害の早期発見及び早期回復については、利用者が対策する必要がある。 仮想マシンを冗長化する場合は、IBM Cloudの冗長構成機能を用いて利用者が実施する必要がある。 仮想マシンの状態やデータのバックアップの作成は、IBM Cloudのレプリケーション機能を用いて利用者が実施する必要がある。
実103	・構成情報をIMS機能により管理しており、障害を検知した場合の切り分け作業に利用可能としています。 ・利用者は、実装するアプリケーションに関して、監視と監視状況に応じた対応を実施する必要があります。 ＜ご参考＞ ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	適合可能	文献[03]の235スライド目にて、災害対策とビジネス継続性のために、IBM Cloudを支える管理システム(IMS)は地理的に分散された冗長性を持っていることを確認した。 文献[09]にて、SOC2の取得証明書を確認した。 なお、SOC2では、IBM Cloudの管理システム(IMS)はインシデント対応とインシデント解決のためのチケット作成および管理の実施について記載されていることを確認した。 また、インタビューにて、障害時などには、IBM Cloudの管理システム(IMS)を利用して障害の切り分けを実施していることを確認した。	要NDA	文献[03] 文献[09]	SOC2　P7 Background	障害時などには、IBM Cloudの管理システム(IMS)を利用して障害の切り分けを実施している。	–	利用者がIBM Cloud上で構築するアプリケーションやサービスの障害の早期発見及び早期回復については、利用者が対策する必要がある。 仮想マシンを冗長化する場合は、IBM Cloudの冗長構成機能を用いて利用者が実施する必要がある。 仮想マシンの状態やデータのバックアップの作成は、IBM Cloudのレプリケーション機能を用いて利用者が実施する必要がある。
実104	・利用者が実装するアプリケーションの障害時の縮退や再構成は、業務に応じて利用者が導入することとしており、対象外とします。 ・IBM Cloudの「クラウド・サービス」(そのシステム、ネットワークおよび基盤となるコンポーネントを含む)は事業継続性および災害復旧の要件について、文書化されたリスク管理ガイドラインに従って個別に評価されます。各IBM「クラウド・サービス」には、当該リスク・アセスメントで保証される範囲において、業界標準の実務に合致する事業継続性および災害復旧の計画が付帯します。 ＜ご参考＞ データのセキュリティおよびプライバシーの原則 SOC2 A1.2, A1.3 ISO 27017 17.2.1 情報処理施設の可用性	適合可能	文献[03]の76スライド目にて、ホストサーバーの物理障害時には、仮想サーバーが他のホストサーバーで起動されるため、可用性を維持できることを確認した。 文献[03]の207スライド目にて、障害時は自動でフェイルオーバー（30秒以内に切り替え）を実施することを確認した。 文献[03]の213スライド目にて、マスタ - マスタ 型でノード障害時もサービスを継続可能であることを確認した。	公開文書	文献[03]	–	–	–	利用者がIBM Cloud上で構築するアプリケーションやサービスの障害の早期発見及び早期回復については、利用者が対策する必要がある。 仮想マシンを冗長化する場合は、IBM Cloudの冗長構成機能を用いて利用者が実施する必要がある。 仮想マシンの状態やデータのバックアップの作成は、IBM Cloudのレプリケーション機能を用いて利用者が実施する必要がある。
実105	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	取引制限機能が必要なアプリケーションやサービスについては、利用者が対策する必要がある。
実106	・利用者が実装するアプリケーションの障害時の縮退や再構成は、業務に応じて利用者が導入することとしており、対象外とします。 ・IBM Cloudの「クラウド・サービス」(そのシステム、ネットワークおよび基盤となるコンポーネントを含む)は事業継続性および災害復旧の要件について、文書化されたリスク管理ガイドラインに従って個別に評価されます。各IBM「クラウド・サービス」には、当該リスク・アセスメントで保証される範囲において、業界標準の実務に合致する事業継続性および災害復旧の計画が付帯します。 ＜ご参考＞ ・データのセキュリティおよびプライバシーの原則 - IBMクラウド・サービス ・SOC2 A1.2, A1.3 ・ISO 27017 17.2.1 情報処理施設の可用性	適合可能	文献[03]の76スライド目にて、ホストサーバーの物理障害時には、仮想サーバーが他のホストサーバーで起動されるため、可用性を維持できることを確認した。 文献[03]の207スライド目にて、障害時は自動でフェイルオーバー（30秒以内に切り替え）を実施することを確認した。 文献[03]の213スライド目にて、マスタ - マスタ 型でノード障害時もサービスを継続可能であることを確認した。 文献[09]にて、SOC2の取得証明書を確認した。 なお、SOC2では、障害時のリカバリ機能について記載されていることを確認した。	公開文書	文献[03] 文献[09]	SOC2 P24　Change Management	–	–	利用者がIBM Cloud上で構築するアプリケーションやサービスの障害の早期発見及び早期回復については、利用者が対策する必要がある。 仮想マシンを冗長化する場合は、IBM Cloudの冗長構成機能を用いて利用者が実施する必要がある。 仮想マシンの状態やデータのバックアップの作成は、IBM Cloudのレプリケーション機能を用いて利用者が実施する必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実107	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実108	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実109	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実110	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実111	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	カードの偽造防止対策が必要なアプリケーションやサービスについては、利用者が対策する必要がある。
実112	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、オープンネットワークを利用した金融サービスの安全性を確保するため、接続相手先が本人であることを確認する予防策やアクセス制限、検知策等の不正使用防止機能を設ける必要がある。 仮想マシン(VM)ロールの場合、お客様は仮想マシンを評価して更新する責任を負う。 加えて、下記のいずれについても、SI事業者あるいは利用者が対応する必要がある。 ・通常とは異なる取引が行われた時等、取引のリスクに応じた更なる本人確認 ・利用者機器（パソコンなど）のシステム環境チェック機能 ・取引内容をモニタリングし、疑わしい取引や異常を検知した場合は取引を一時的に中断する仕組み ・ハードウェアトークン等を利用したトランザクション認証
実113	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、利用者自身が使用状態を確認する機能を設ける必要がある。
実114	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実115	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実116	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実117	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。
実118	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者がIBM Cloud上で構築する環境については、利用者が対策する必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実119	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、無人店舗におけるセキュリティ及び安定運用に関わる対策を講ずる必要がある。
実120	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、無人店舗におけるセキュリティ及び安定運用に関わる対策を講ずる必要がある。
実121	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、無人店舗におけるセキュリティ及び安定運用に関わる対策を講ずる必要がある。
実122	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、無人店舗におけるセキュリティ及び安定運用に関わる対策を講ずる必要がある。
実123	利用者による実施内容のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、無人店舗におけるセキュリティ及び安定運用に関わる対策を講ずる必要がある。
実124	CD/ATMおよび無人店舗の管理は利用者の管理事項となります。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、無人店舗におけるセキュリティ及び安定運用に関わる対策を講ずる必要がある。
実125	インストアブランチに関する事項であり、対象外となります。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、サービスにおける安全利用を考慮し出店先等の選定基準を明確にする必要がある。
実126	コンビニATMに関する事項であり、対象外となります。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、サービスにおける安全利用を考慮し出店先等の選定基準を明確にする必要がある。
実127	コンビニATMに関する事項であり、対象外となります。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、サービス利用機器メンテナンスにおける防犯体制及び防犯方法を明確にする必要がある。
実128	コンビニATMに関する事項であり、対象外となります。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、サービス利用において障害時・災害時の対応手順を明確にする必要がある。
実129	コンビニATMに関する事項であり、対象外となります。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、サービス利用機器における伝送データの安全対策等を講ずるが必要がある。
実130	コンビニATMに関する事項であり、対象外となります。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、サービスにおける安全利用を考慮し各種関係者との連絡体制を明確化する必要がある。
実131	コンビニATMに関する事項であり、対象外となります。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、サービスにおける安全利用を考慮し顧客への注意喚起を行う必要がある。
実132	デビットカード・サービスに関する事項であり、対象外となります。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、サービスにおける安全利用を考慮し各種関係者と安全対策を講ずる必要がある。
実133	デビットカード・サービスに関する事項であり、対象外となります。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、サービスにおける安全利用を考慮し各種関係者と安全対策を講ずる必要がある。
実134	デビットカード・サービスに関する事項であり、対象外となります。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、サービスにおける安全利用を考慮し各種関係者と安全対策を講ずる必要がある。

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
実135	デビットカード・サービスに関する事項であり、対象外となります。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、サービスにおける安全利用を考慮し顧客への注意喚起を行う必要がある。
実136	前払式支払手段に関する事項であり、対象外となります。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、顧客に対して、媒体等の紛失/盗難/破損等により顧客が被る可能性のある損害及びこれらに対する顧客の責任について、明示する必要がある。
実137	前払式支払手段に関する事項であり、対象外となります。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	電子的価値の保護機能が必要なアプリケーションやサービスについては、利用者が対策する必要がある。
実138	電子メールの運用方針の明確化は利用者の管理事項であり、対象外となります。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	IBM Cloud上に利用者により構築するメールサービスについての運用方針については、利用者により明確にする必要がある。
実139	電子メール、ホームページ閲覧の運用方針の明確化は利用者の管理事項であり、対象外となります。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	業務目的以外の電子メールの送受信やホームページの閲覧等については、利用者が対策する必要がある。
実140	顧客の認証は利用者による管理領域であり、対象外となります。 生体情報は、機密情報と位置づけ、取扱いに関しては、利用者との間で定められた、態勢、手続き、手順に則り、管理責任者を定めます。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、生体認証情報を用いる場合、安全に管理するための必要な手順を定める必要がある。
実141	顧客の認証は利用者による管理領域であり、対象外となります。 生体情報は、機密情報と位置づけ、取扱いに関しては、利用者との間で定められた、態勢、手続き、手順に則り、管理責任者を定めます。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者がIBM Cloud上で構築するアプリケーションやサービスで独自に生体認証を用いる場合は、利用者が適切な対策を行う必要がある。
実142	金融機関内部の統制のため対象外としました。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、IBM Cloud上でQRコード決済機能を含むアプリケーションを実装する場合、安全対策の措置を講ずる必要がある。
実143	金融機関内部の統制のため対象外としました。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、IBM Cloud上でQRコード決済機能を含むアプリケーションを実装する場合、顧客保護の措置を講ずる必要がある。
実144	金融機関内部の統制のため対象外としました。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	利用者は、IBM Cloud上でQR コード決済機能を含むアプリケーションを実装する際、利用上の留意事項を顧客に明示する必要がある。
設1	IBM Cloudは"Uptime Institute Tier3"以上のデータセンターで運用されています。詳細はIBMにお問い合わせください。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設2	IBM Cloudは"Uptime Institute Tier3"以上のデータセンターで運用されています。詳細はIBMにお問い合わせください。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
設3	建物基準法に記載されている通り、敷地内の適正な経路を確保することができます。 <ご参考> ・IBM Cloudのレギュレーション対応 ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設4	最も近い隣接ビルへの距離は 10m を超えています。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設5	データセンターの建物は24時間監視体制のもと、データセンター周辺の公道から警備員を配置しています。建物への入館には必ず受付を通る必要があり、建物内の共通のエリアにはさらに入館チェックを通過する必要があります。 IBM は、「クラウド・サービス」のホストに使用されるIBM 施設（データセンター）への不正な入場から保護するため、適切に物理的な入場管理（柵、カード制御の入口、監視カメラ、および有人の受付デスクなど）を維持管理します。データセンターへの補助的な入口（配達エリアおよび発送センターなど）は管理され、コンピューティング・リソースから隔離されます。 <ご参考> ・IBMクラウド・セキュリティガイドブック ・IBMクラウド・サービスのデータのセキュリティーおよびプライバシーの原則	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設6	ISO 27017 (ISO 27002 11.1.3 オフィス，部屋及び施設のセキュリティ「建物を目立たせず，その目的を示す表示は最小限とし，情報処理活動の存在を示すものは，建物の内外を問わず，一切表示しない。」)に準拠し、適合可能と解釈します。 どの種類のコンピューター・センターも存在することを示す署名はありません。 <ご参考> IBM Cloudのレギュレーション対応	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設7	詳細はIBMにお問い合わせください。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設8	それぞれのデータセンターは複数のサーバールームを保持しており、サーバールームはデータセンター内にて別のエリアとして設計されています。 詳細はIBMにお問い合わせください。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設9	ISO 27001 11.2.3 ケーブル配線のセキュリティ「データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は，傍受，妨害又は損傷から保護する。」に準拠し、適合可能と解釈します。 電気ユーティリティ XLPE ケーブルは、地下から直接データセンターの直下に直接、地下には地下 10m 以上の地下ケーブルから直接接続しています。通信ケーブルは、既存のケーブルによる偶発的な損傷を防止するために、慎重に調整されます。 <ご参考> IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
設10	詳細はIBMにお問い合わせください。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設11	詳細はIBMにお問い合わせください。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設12	詳細はIBMにお問い合わせください。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設13	詳細はIBMにお問い合わせください。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設14	詳細はIBMにお問い合わせください。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設15	詳細はIBMにお問い合わせください。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設16	出入設備管理については、有人による受付管理を行っています。 <ご参考> ・IBM Cloud セキュリティガイドブック https://www.ibm.com/downloads/cas/DG5Q0DRA	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応						SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
設17	緊急ドアには、避難を容易にするためのコードに対応したパニック・オープン・デバイスが備えられており、緊急ドア・リリースによって起動される「ドア強制オープン」アラームが出されています。 〈ご参考〉 IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB IBM SECMAN https://w3-03.ibm.com/security/secweb.nsf/ObjectFileDocView/IBM+Security+Manual+2019+--+11012019(finalv3).pdf/$File/IBM+Security+Manual+2019+--+11012019(finalv3).pdf	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設18	IBM は、「クラウド・サービス」の物理的インフラストラクチャーを、自然発生的および人為的な環境脅威（極端な周辺温度、火災、洪水、湿度、窃盗、および破壊行為など）から保護するための予防措置を講じています。 この建物は洪水レベルと津波/潮汐のサージ・レベルの上にあり、すべての基礎レベルの開口部にはポンプやその他の排水システムが必要とされています。 SOC2 Report H4「Data centers facilities are protected against environmental factors such as fire, water, and heat」に準拠し、適合可能と解釈します。 Physical and Environmental Protection Policy「5.2 Water Damage Protection」をインタビューで確認し、適合可能と解釈します。 〈ご参考〉 ・IBMクラウド・サービスのデータのセキュリティおよびプライバシーの原則： https://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設19	IBM SECMAN に記載があります。詳細はIBMにお問い合わせください。 全出入口に十分な強度を備えた防火ドア・シャッターが設置されています。 〈ご参考〉 IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB IBM SECMAN https://w3-03.ibm.com/security/secweb.nsf/ObjectFileDocView/IBM+Security+Manual+2019+--+11012019(finalv3).pdf/$File/IBM+Security+Manual+2019+--+11012019(finalv3).pdf	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設20	建築基準法と消防法の両方に準拠して、耐火性・耐火性のある材料を使用しています。 〈ご参考〉 IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設21	IBM は、「クラウド・サービス」の物理的インフラストラクチャーを、自然発生的および人為的な環境脅威（極端な周辺温度、火災、洪水、湿度、窃盗、および破壊行為など）から保護するための予防措置を講じています。 また、内部の金具や毛皮は地震に対して固定され、硬化しており、建物自体もシーズミカルに分離されています。 〈ご参考〉 ・IBMクラウド・サービスのデータのセキュリティおよびプライバシーの原則 https://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
設22	ISO 27017 (ISO 27002 11.1.4 外部及び環境の脅威からの保護「火災，洪水，地震，爆発，暴力行為，及びその他の自然災害又は人的災害からの損傷を回避する方法について，専門家の助言を得た上で物理的な保護を設計する」)に準拠し、適合可能と解釈します。 シーズミック・ショックを軽減するために、地震分離層の上にコンピューター室が設置されています。 また、各コンピューター室はそれぞれ別の消防地帯となっており、隣接する場所での火災の影響を受けない可能性が高いということです。 〈ご参考〉 IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ISO 27017	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設23	詳細はIBMにお問い合わせください。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設24	サーバールームの出入り口のドアには施設を特定できるような表示は出ておらず、公開エリアに面した出入り口は1つも存在しません。 〈ご参考〉 IBMクラウド・セキュリティ https://www.ibm.com/downloads/cas/DG5Q0DRA	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設25	コンピューター室内のレイアウト設計と実装は、運用アクセスと保守アクセスの両方のためのスペースを考慮に入れました。 〈ご参考〉 IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設26	詳細はIBMにお問い合わせください。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設27	コンピューター・ルームごとに 1 つの通常の入り口があり、ID カード読取装置によって制御されます。 また、それぞれの部屋には、熱、湿度、およびほこりの摂取を減らすためのアンテルームがあります。 〈ご参考〉 IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設28	詳細はIBMにお問い合わせください。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–

FISC安全対策基準（第9版改訂）の項目 項番	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応 FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
設29	IBM SECMAN に記載があります。詳細はIBMにお問い合わせください。 コンピューター室などの重要な部屋には窓が全くありません。 <ご参考> IBM SECMAN https://w3-03.ibm.com/security/secweb.nsf/ObjectFileDocView/IBM+Security+Manual+2019+-+11012019(finalv3).pdf/$File/IBM+Security+Manual+2019+-+11012019(finalv3).pdf IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
設30	建物基準法と消防法によって、緊急出口、避難装置、誘導灯が設置されています。 <ご参考> IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設31	各コンピューター・ルームは、建物基準法に従って独立した発火区画として定義されています。 <ご参考> IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設32	SOC2 Report H4「Data centers facilities are protected against environmental factors such as fire, water, and heat」に準拠し、適合可能と解釈します。 Physical and Environmental Protection Policy「5.2 Water Damage Protection」をインタビューで確認し、適合可能と解釈します。 機械の回廊には防水床、バンディング、漏水検出テープ、および緊急排水が存在します。 <ご参考> IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB SOC2 Report H4「Data centers facilities are protected against environmental factors such as fire, water, and heat」に	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設33	詳細はIBMにお問い合わせください。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設34	コードに準拠した非可燃性およびフレイムの材料が使用されます。 <ご参考> IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設35	コンピューター室の区画の壁は、落下を防ぐために、床と天井のスレッズに固定されています。 また、天井はペアスラブで、天井板を使用した天井のスラブ・アンカーは、地震用の腕輪を使用して照明用のレースウェイを吊り下げます。 <ご参考> IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設36	上げ床タイルは、タイルが減少し、タイルに損傷を与えることを防ぐために、台座にボルトで固定されます。 <ご参考> IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設37	詳細はIBMにお問い合わせください。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
設38	IBM Cloudは"Uptime Institute Tier3"以上のデータセンターで運用されています。詳細はIBMにお問い合わせください。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設39	詳細はIBMにお問い合わせください。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設40	ISO 27001 11.2.3 ケーブル配線のセキュリティ「データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は，傍受，妨害又は損傷から保護する。」に準拠し、適合可能と解釈します。 すべてのケーブルは炎のリターダントで、すべての火災ゾーンの侵入は停止しています。 〈ご参考〉 IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設41	詳細はIBMにお問い合わせください。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設42	Physical and Environmental Protection Policy「4.3 Emergency Lighting」をインタビューで確認し、適合可能と解釈します。 コンピューター室にはコードに準拠した緊急照明があります。 〈ご参考〉 IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設43	コンピューター室内での水使用設備は、いかなる場合も許容されていません。 〈ご参考〉 IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設44	詳細はIBMにお問い合わせください。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応						SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
設45	詳細はIBMにお問い合わせください。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設46	詳細はIBMにお問い合わせください。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設47	健康や安全上のコードで求められるとおり、適切な防犯対策がとられています。 〈ご参考〉 IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設48	詳細はIBMにお問い合わせください。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設49	すべての金属面は保税され、接地され、湿度は 40 から 55% RHの間で維持されています。 〈ご参考〉 IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設50	詳細はIBMにお問い合わせください。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設51	カートおよびその他のホイール付きデバイスには、ブレーキやロックがあります。 〈ご参考〉 IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設52	ISO 27017 (ISO 27002 11.1.4 外部及び環境の脅威からの保護「火災，洪水，地震，爆発，暴力行為，及びその他の自然災害又は人的災害からの損傷を回避する方法について，専門家の助言を得た上で物理的な保護を設計する」)に準拠し、適合可能と解釈します。 電気・機械室は、外部からの火災や地震の被害を受ける危険のない、地震による安全な場所に位置しています。 〈ご参考〉 IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
設53	コードに準拠した避難および作業スペースは、機器周辺で保護されています。 <ご参考> IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設54	IBM SECMAN に記載があります。詳細はIBMにお問い合わせください。 重要なインフラストラクチャー・ルームとコンピューター・ルームは、別々の部屋にあります。 物理的なアクセスは、各施設とサーバールームのキーカード近接システムを通じて制御されます。電気、発電機、UPS、バッテリー、消火用配管/スプリンクラー、HVAC機器などの重要性の高いエリアを含む各施設へのアクセスおよび各施設全体へのアクセスは制限され、サーバールームへのアクセスは許可された担当者に制限されます。 <ご参考> IBM SECMAN https://w3-03.ibm.com/security/secweb.nsf/ObjectFileDocView/IBM+Security+Manual+2019+–+11012019(finalv3).pdf/$File/IBM+Security+Manual+2019+–+11012019(finalv3).pdf IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB Security Manual SOC2 Report Physical Security	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設55	物理的なアクセスは、各施設とサーバールームのキーカード近接システムを通じて制御されます。電気、発電機、UPS、バッテリー、消火用配管/スプリンクラー、HVAC機器などの重要性の高いエリアを含む各施設へのアクセスおよび各施設全体へのアクセスは制限され、サーバールームへのアクセスは許可された担当者に制限されます。 <ご参考> IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB SOC2 Report Physical Security	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設56	詳細はIBMにお問い合わせください。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設57	詳細はIBMにお問い合わせください。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設58	詳細はIBMにお問い合わせください。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・Tier Classification System, Uptime Institute https://uptimeinstitute.com/tiers ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
設59	Physical and Environmental Protection Policy「5.2 Water Damage Protection」 機械の回廊には防水床、バンディング、漏水検出テープ、および緊急排水が存在します。 <ご参考> IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB Physical and Environmental Protection Policy	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設60	・壁面の貫通部分には防火措置を講じている。またIBM Cloud の各データセンターの扉は全て充分な強度を有する防火扉となっている。 すべてのペネトレーションは、火災の壁面と同じ評価に対して適切に起動されます。 <ご参考> ・ IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設61	・機器諸元に対し余裕のある容量を確保するとともに、コンピュータ室の電力使用状況を定期的に確認し、定格の80%をしきい値として設備増設要否の判断を実施しています。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設62	・本線、予備線および予備電源線の 3系統で受電しています。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設63	・CVCF機能を持つUPS設備を設置しています。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設64	・自家発電機および蓄電池設備（UPS）を設置しています。 ・発電機の燃料は連続24時間程度の運転が可能な量を保有しており、月次で無負荷による稼働確認を行っています。 ・UPSは定格で10分間の給電が可能です。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設65	・避雷器（サージアレスタ）およびUPS（CVCF機能）を設置しています。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
設66	・スラブ（コンクリート床）への直接固定や転倒防止器具の設置による耐震措置を講じている。 すべての電源機構は、関連するコードおよび標準に完全に準拠しているチャネル・ベースを使用して、フロア・スレブに固定されています。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	－	－	－	－	－	－
設67	・コンピュータ機器への電源は専用分電盤から専用回路にて配線しています。 コンピューター・デバイスへの電力配分ボードは、専用と冗長の両方になります。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	－	－	－	－	－	－
設68	・コンピュータ機器および負荷変動の激しい機器への電源は、高圧変圧器より分離する措置を講じています。 コンピューター・システムへの電源機構は、専用の UPS システムから提供されます。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	－	－	－	－	－	－
設69	・サーバラック筐体のアースはそれぞれ別個に接地端子盤まで配線しています。 コンピューター・システムに対する専用の接地が施工されています。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	－	－	－	－	－	－
設70	・法令および自社の技術基準に基づき過電流を遮断するブレーカ容量を設計するとともに、漏電警報装置を設置しています。 ・過電流によるUPS装置の故障に備えバイパス回路を設置しています。 接地レーカのアラームと過電流回路ブレーカーが取り付けられています。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	－	－	－	－	－	－
設71	・防災、防犯設備用に予備電源を設置しています。 文献[データのセキュリティーおよびプライバシーの原則 – IBMクラ ウド・サービス]においても、「自然発生的および人為的な環境脅威（極端な周辺温度、火災、洪水、湿度、窃盗および破壊行為など）などから保護するための予防措置を講じることを明記しています。 〈ご参考〉 ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	－	－	－	－	－	－

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
設72	・機器諸元に対し余裕のある能力を確保しています。 ・コンピュータ室の温湿度を定期的に確認し、設備増設や設定値を判断する材料としています。 ・施設内には機器増設に備えた余剰スペースを確保しています。 ISO 27017 (ISO 27002 11.2.2 サポートユーティリティ「事業の成長及び他のサポートユーティリティとの相互作用に対応する能力を，定期的に評価する」)に準拠し、適合可能と解釈します。 コンピューター室専用の機械的回廊に、CRAH ユニットを設置するための追加スペースがあります。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設73	・外気取り入れ口にフィルタを設置し、塵埃等の侵入を防止しています。 ・空調ダクトの設計に際してショートサーキットの防止を考慮しています。 ISO 27017 (ISO 27002 11.2.2 サポートユーティリティ「適切に機能することを確実にするために，定期的に検査及び試験する」)に準拠し、適合可能と解釈します。 外気換気および湿度制御のための専用 AHU が取り付けられています。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設74	・コンピュータ室専用に空調設備を設置しています。 加熱および冷却（HVAC）メカニズムとして、コンピュータルーム空調（CRAC）ユニット、コンピュータルームの空気調和機（CRAH）、冷却水循環装置、および温湿度の監視と制御を備えています。 すべての CRAHS は、1 台のコンピューター・ルーム専用です。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance ・SOC2 Report Environmental Controls	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設75	・空調機の予備をホットスタンバイにて運用しています。 ・IBM Cloudでは、Tier3以上のデータセンターで運用されています。なお、米国発の基準であるTierを日本向けにした、日本版Tierともいうべき指標は、日本独自の要素（地震、津波や火事）を加えたものとして公開されています。 ・Tier3の建物、電機設備項目にて対応しています。 <ご参考> ・IBM Cloudのレギュレーション対応 https://www.ibm.com/downloads/cas/O5WEZQAB ・SoftLayer Technologies, Inc.' s Infrastructure as a Service (IaaS) SOC 2 Report Relevant to the Security and Availability Criteria ・ISO 27001 ・Cloud Security Alliance	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設76	・空調温湿度の自動制御を行うとともに、温度の設定値逸脱や設備異常時には警報を発報し、手動運転への切り替えを可能としています。 空調装置には、自動制御装置、緊急警報装置があり、BMSを使用してリモート側でモニターおよび操作されています。 装置のすべての障害または障害が原因で、スタンバイ装置の手動または自動始動が行われます。 <ご参考> ・IBMクラウド・セキュリティガイドブック ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・ IBM Cloudのレギュレーション対応 ・A guide to IBM Bluemix resiliency and security	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応						SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
設77	・空調設備は施錠した専用室に設置しています。 空調装置が配置されているメカニカル・コリダーはロックされており、取り外し可能なドアハンドルがあります。 〈ご参考〉 ・IBMクラウド・セキュリティガイドブック ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・ IBM Cloudのレギュレーション対応 ・A guide to IBM Bluemix resiliency and security	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設78	・耐震対策として空調設備を設備架台に固定しています。 ・配管やダクトに振れ止めを設置するとともに、免震装置の境界には伸縮継手（ボールジョイント）を使用しています。 CRAH ユニットは床の研究室に適切に固定されています。 〈ご参考〉 ・IBMクラウド・セキュリティガイドブック ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・ IBM Cloudのレギュレーション対応 ・A guide to IBM Bluemix resiliency and security	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設79	・空調ダクトには断熱材を、吸排気口には不燃材料を使用しています。 コンピューター室内の断熱材および空気吸気口は、すべて不燃性です。 〈ご参考〉 ・IBMクラウド・セキュリティガイドブック ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・ IBM Cloudのレギュレーション対応 ・A guide to IBM Bluemix resiliency and security	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設80	・空調や電源設備の稼働状況、負荷状況の監視装置を中央管理室に設置しています。 〈ご参考〉 ・IBMクラウド・セキュリティガイドブック ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・ IBM Cloudのレギュレーション対応 ・A guide to IBM Bluemix resiliency and security	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設81	・コンピュータ室や設備機械室から独立した中央管理室を設置し、空調や電源設備の稼働状況など法令に従った監視を行っています。 ・法令（建築基準法施行令）に従った形で中央管理室を設置し、役割を定めています。 ・中央管理室では、次の設備等について限界設定および監視を行っています。 ・CVCF ・蓄電池 ・自家発電 ・給排水 ・消火設備 ・監視設備 ・通信回線 〈ご参考〉 ・IBMクラウド・セキュリティガイドブック ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・ IBM Cloudのレギュレーション対応 ・A guide to IBM Bluemix resiliency and security	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設82	・回線の機器収容部分はカードキー（電気錠）により施錠を行い、開錠時のログを取得して保存しています。 ISO 27017 (ISO 27002 11.2.3 ケーブル配線のセキュリティ「外装電線管の導入。点検箇所・終端箇所の施錠可能な部屋又は箱への設置」)に準拠し、適合可能と解釈します。 関連するすべてのスペースは、ロックまたは電子制御されます。 〈ご参考〉 ・IBMクラウド・セキュリティガイドブック ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・ IBM Cloudのレギュレーション対応 ・A guide to IBM Bluemix resiliency and security	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設83	・回線関連設備の設置場所の表示は行っていません。 〈ご参考〉 ・IBMクラウド・セキュリティガイドブック ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・ IBM Cloudのレギュレーション対応 ・A guide to IBM Bluemix resiliency and security	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
設83-1	・MDF（主配電盤）室を複数箇所設け、専用の配線スペースを確保しています。 ・コンピュータ室内では、電源ケーブルと通信ケーブルを隔離して配線しています。 (ISO 27002 11.2.3 ケーブル配線のセキュリティ「配線盤，端子盤及びケーブル室への管理されたアクセス」)に準拠し、適合可能と解釈します。 Diverse MDF（メイン配布フレーム）室は、建物のエントリー・ポイントからコンピューター・ルームまでのすべての方法で、完全に多様な経路を提供するために取り付けられています。 <ご参考> ・IBMクラウド・セキュリティガイドブック ・技術よりな人が最初に読む:IBMCloud柔らか層本 ・ IBM Cloudのレギュレーション対応 ・A guide to IBM Bluemix resiliency and security ISO 27017	評価中	対策状況の詳細についてはIBMへ確認	–	–	–	–	–	–
設84	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	–
設85	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	–
設86	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	–
設87	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	–
設88	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	–
設89	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	–
設90	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	–
設91	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	–
設92	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	–
設93	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	–
設94	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	–
設95	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	–
設96	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	–
設97	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	–
設98	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	–
設99	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	–	–	–	–	–	–

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応						SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
設100	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設101	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設102	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設103	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設104	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設105	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設106	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設107	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設108	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設109	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設110	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設111	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設112	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設113	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設114	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設115	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設116	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設117	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設118	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設119	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設120	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－

FISC安全対策基準（第9版改訂）の項目	FISC安全対策基準（第9版改訂）に対するIBMの見解	IBM Cloudにおける対応							SI事業者・利用者で必要な対応
項番		FISC安全対策基準への適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	IBMへのインタビューで確認した内容	NDAに基づき確認した資料	
設121	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設122	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設123	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設124	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設125	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設126	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設127	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設128	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設129	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設130	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設131	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設132	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設133	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設134	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設135	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設136	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
設137	利用者の本部、営業店等の要件のため対象外とします。	対象外	金融機関内部の統制のため対象外	－	－	－	－	－	－
監1	・ISO27001、FedRAMP、FISMA、HIPAA等の認証のための外部監査を定期的に実施しています。 <ご参考> ・技術よりな人が最初に読む:IBMCloud柔らか層本	適合可能	文献[03]の235スライド目にて、IBM社員業界標準ポリシーと行動に対して教育が実施され、毎年監査されていることを確認した。 文献[03]の239スライド目にて、第三者による監査業者が継続的に監査を実施していることを確認した。 文献[02]の「1. データ保護 c」にて、要求に応じて、IBM は、TD（取引文書）に特定された適格な独立した第三者による監査 (ISO 27001、SSAE SOC 2 等) による証明書、認証、報告書といった遵守および認定の証拠を提出することを確認した。	公開文書	文献[02] 文献[03]	－	－	－	利用者は、システム監査体制を整備する必要があり、必要に応じて監査レポートの確認、監査担当者への質疑応答等を行う必要がある。