IBM Cloudのレギュレーション対応

オンプレミス、オフプレミス、ハイブリッドあるいはマルチのいずれのクラウドであろうと、セキュリティーの確保は最優先事項です。例えば、クラウド上に新たなシステムを構築してサービス提供する場合、その企業は、どの程度自社のセキュリティー要件を満たせるのか、満たせないものがあればどう対応する必要があるかを判断し、対策を講じなければなりません。IBMは「IBM Cloud」のセキュリティーがお客様要件に合致するか確認できるよう、IBM Cloudで実装されているセキュリティーに関する情報を公開しています。

本稿では、クラウドにおけるセキュリティーの基本的な考え方、IBM Cloudにおける代表的な各種レギュレーションやGDPRへの対応について紹介します。

1. クラウドにおけるセキュリティーの基本的な考え方

クラウドのセキュリティーは責任共有モデルである、とよく表現されます。利用者自身で制御できる部分と、クラウド事業者に一任する部分の組み合わせによってシステムが成り立っているのがその主な理由です（**図1**）。

IBM Cloudでは、**図1**の実線枠部分にお客様のポリシーを適用しやすいように、さまざまな機能を利用できます。例えばIaaSでは管理者権限が利用できるので、お客様指定のセキュリティー・ツールを導入することができます。また点線枠部分は、「NIST 800-53 framework」[1]を基準とした米国政府標準に従って提供されています。さらに、これまでオンプレミスでお客様自身が実施してきたのと同等以上のセキュリティー・ポリシーが適用され、適切に運用されていることがいつでも確認できるように、第三者機関による監査レポートなどが提供されています。

クラウドの検討はIaaSから取りかかることが多く、まずはインフラ要件を検討する必要があります。また、クラウド登場までのオフプレミスの選択肢の主流の一つであったホスティングやハウジング選択時のセキュリティー・チェックは、設備面に関するものが多くありました。次章では、データセンター設備についての傾向を見てみましょう。

2. IBM Cloudデータセンターの採用基準

データセンター選定の主要な基準として、米国の信頼性基準でもある「Tier Performance Standards」[2]がよく知られています。Tierは、データセンターに要求

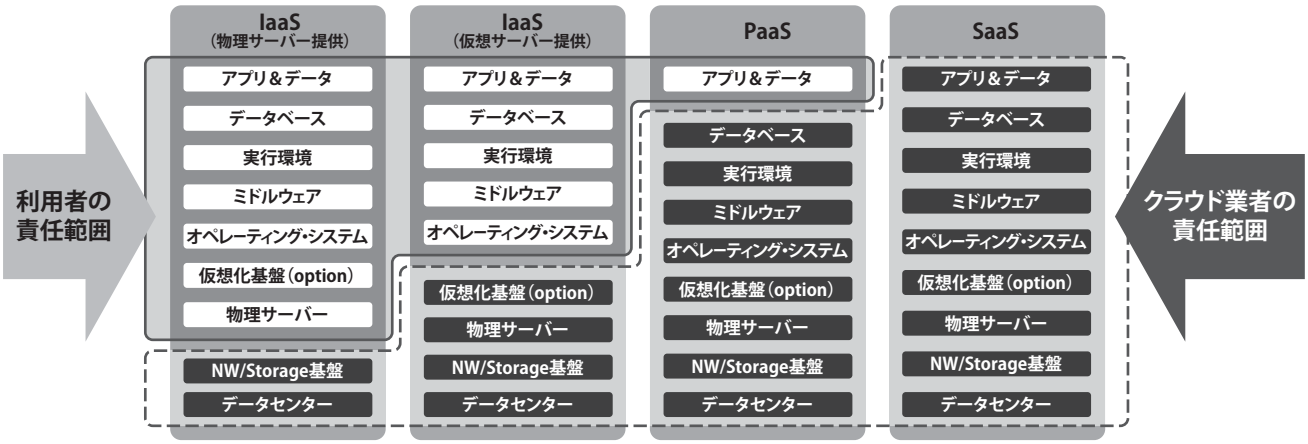

図1. クラウドの利用形態（IaaS/PaaS/SaaS）の違いにおける責任分界点

されるパフォーマンス・レベルに合わせてデータセンター設備をTier1からTier4の4つの階層に分類したもので（**図2**）、立地条件や建物そのものの堅牢性、電力や回線の経路、電源容量、無停電電源の配置状況、運用者といったスタッフの配置など、さまざまな観点で評価されたものです。セキュリティーというよりは冗長構成などの信頼性に大きく影響する評価項目が多くなっています。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[3]。

3. IBM Cloudで取得している代表的なレギュレーション

IBM CloudではISO27001、ISO9001、PCIなど多くの国際標準に準拠するだけではなく、米国、欧州、日本、シンガポールなど国別に定められた各種のレギュレーションやコンプライアンスに対応しています[4]。

本章では、代表的なレギュレーションの中でもクラウドそのものを保障するものとしてよく参照されるSOC（Service Organization Control）レポートに注目してみましょう。SOCレポートとは、米国公認会計士協会（AICPA）が整理したフレームワークで、SOC1、SOC2、SOC3の3種に大別されます。SOC1は主に財務報告に関連する内部統制に関する保証報告書、SOC2は主に財務報告以外（セキュリティー、信頼性、可用性、プライバシーなど）に関連する内部統制に関する保証報告書、SOC3はSOC2と同様の項目をカバーし、マーケティング目的で受託会社が公的に使用できる短めのレポートです。

SOC1、SOC2には、それぞれにType1、Type2があります。Type1は基準日時点での記述書の記載の妥当性や内部統制のデザイン、適用の妥当性を評価し保証するのに対して、Type2ではType1の評価、保証に加えて一定期間の運用状況の有効性も評価し、保証されます。

SOC1およびSOC2はその特性上、年1回更新されるべきレポートです。クラウドのSOCレポートとして妥当なのは、セキュリティー、信頼性、可用性、プライバシーなどに関連する報告書であり、一定期間の運用状況が評価・保障されたものである、SOC2 Type2レポートです。IBM Cloudの利用者は、管理者ポータルから年1回更新されているSOC2 Type2レポートの参照を申請することができます。

4. 業界別の代表的レギュレーション

業界によって順守すべきレギュレーションはさまざまです。本章では、金融業界、医療業界におけるレギュレーションについて説明します。

4-1. 金融業界

4-1-1. IT動向とクラウド・セキュリティー

金融（Finance）と技術（Technology）を融合させたFinTechが浸透し、銀行法改正による電子決済等代行業に関する法整備も進むなど、金融機関を取り巻く環境は急速に変化を続けています。同時に金融関連システムとしてのセキュリティーやプライバシーの重要性がますま

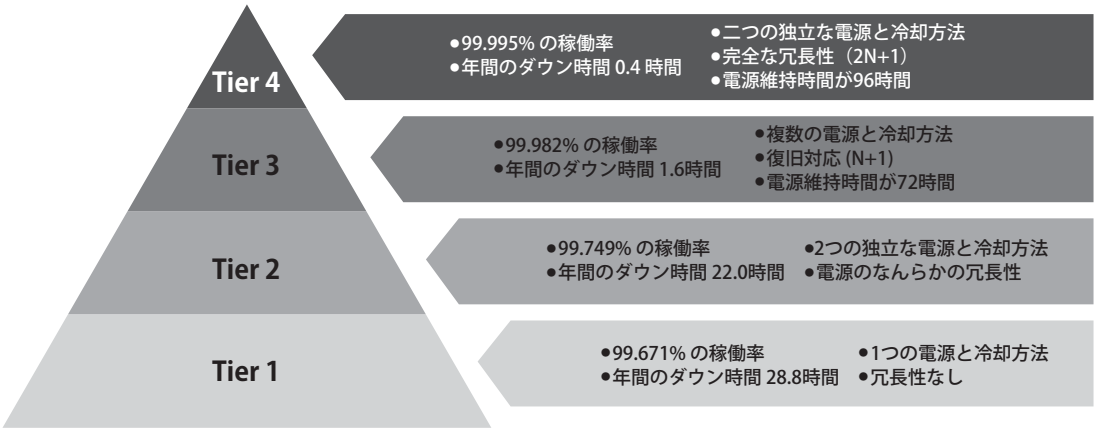

図2. Tier Performance Standardsの指標

す高まっています。モバイル、IoT、オープンAPI、ブロックチェーン、ビッグデータやAI、RPA(ロボティクス・プロセス・オートメーション)などを活用したデジタル・イノベーション、自動化、キャッシュレス化、さらには働き方改革に至るまで、変化への柔軟性と俊敏性がサービス向上や競争力強化に欠かせないものとなってきました。ITプラットフォームとしてクラウドを活用することで、サービスの展開や撤退が容易になり、最新技術への追従、コスト効率の向上、外部連携によるオープン・イノベーション推進などの効果が期待されています。

一方で、クラウドを活用することによる金融サービスとしての安全性・信頼性に影響があるのではないかという不安が障壁となる場合があります。クラウド活用は、外部委託の一形態と考え、その透明性の確認や責任分界点、監督責任の明確化、広帯域ネットワーク利用に伴うサイバー・アタック対策など、クラウド活用による新たな脅威、リスクへの対応を適切なレベルで講じることが重要となります。この際に、FISC安全対策基準や、この基準に対するクラウドの評価レポートを活用できます。

4-1-2. FISC安全対策基準

FISC安全対策基準は日本における金融情報システムに関する安全対策の自主基準で、正式名称は、公益財団法人 金融情報センター(FISC) 発刊の「金融機関等コンピュータシステムの安全対策基準・解説書」です。金融庁による監査もこの基準が参照されており、事実上の業界標準ガイドラインとなっています。

1985年に初版が策定されて以来33年間で第9版まで改訂されています。2011年第8版ではインターネットWebに対応した改訂がなされ、2013年第8版追補ではクラウド、モバイル、震災、標的型攻撃対策、CSIRT(Computer Security Incident Response Team)整備などの対応が追補されました。2015年第8版追補改訂ではサイバー攻撃対応、クラウド利用に関して捕捉されています。その後、FinTechの活用などを踏まえ、外部統制やリスクベース・アプローチの導入など行い、章立てを大きく見直した第9版が2018年3月に発刊されました[5]。

4-1-3. IBM CloudにおけるFISCガイドラインへの対応

IBMでは、FISC安全対策基準(第8版、第8版追補改訂)に基づいてIBM Cloudの適合性について自己評価を実施、さらに第三者による確認として外部監査法人による調査を実施し、その結果を公開しています[6]。第9版への対応版は、2018年10月時点で発行準備中です。

表1はIBM Cloud インフラストラクチャー・サービス(IaaS)の評価結果サマリーです。他にIBM Cloudプラットフォーム・サービス(PaaS)の評価も実施しています[7]。これらの評価を通じて、設備、運用、技術の各項目に対して、クラウド・サービスとして対応すべき項目は全て基準を満たしていることが確認されました。また、IaaSとしては対象外となる項目(**表1**でN/Aの列)についてもIBMの運用支援、アプリケーション開発などのサービスを付加することで対応可能であることが確認できて

表1. IBM Cloudインフラストラクチャーの FISC安全対策基準評価サマリー

基準項目	項目数	○	△	N/A
設備基準	84※	84	0	0
運用基準	120	61	0	59
技術基準	53	28	0	25

○：現時点では安全対策基準を満たしていると判断できる項目
△：安全対策の強化について検討中ないし検討予定のある項目
N/A：提供サービス(IaaS)の対象外と判断した項目

※設84以降は、本部・営業店等、流通小売店舗との提携チャネルを対象とした項目のため、本調査では対象外としています。

表2. IBM運用支援、アプリケーション開発サービスでのカバー範囲

基準項目	項目数	運用支援サービス追加で対応	アプリ開発サービス追加で対応	運用支援&アプリ開発サービス追加で対応	ITベンダー提供の領域外※
設備基準	84	N/A=0			
		0	0	0	0
運用基準	120	N/A=59			
		16	2	15	26
技術基準	53	N/A=25			
		1	9	12	3

※CD、ATMおよび無人店舗、カード管理、営業店、コンビニATM等の金融機関機器や現物管理関連の項目が対象外となります。

います（**表2**）。

このように、IBM Cloudを利用することで、対象システムのセキュリティー要件に応じて、適切なリスク・レベルでFISC安全対策基準に準拠したシステムの構築が可能です。

4-2. 医療業界

4-2-1. IT動向とクラウド・サービスの活用

日本の医療分野における情報技術の活用は、1970年代から普及した医療事務や診療を支援するシステムに始まり、昨今では、AIの技術を活用した画像診断、IoTデバイスを活用した患者の健康状態の把握、医療機関間の情報共有による遠隔地からの医療サービス提供、電子処方箋の運用実証などが挙げられます。超高齢化社会を迎える日本において、これらの新しい取り組みにより、医療現場の人材不足、医療サービスへの需要増加、医療費増加といった課題を解決し、安全で良質かつ効率的な医療サービスを実現することが重要となっています。一方で、患者の医療情報は極めて個人的な情報であり、個人の社会的な評価等に関わるおそれもあるため、医療分野における情報化、外部委託、他サービスとの連携などの進展に伴い、その情報の保護および医療情報システムの安全管理がよりいっそう必要とされています。

すなわち医療サービスを支援するITプラットフォームには、医療情報の安全な収集・保管・分析・通信・廃棄を大前提として、増大するデータの種類および容量への柔軟な対応、外部との円滑かつセキュアな情報連携、IoTやAIといった新しい情報技術の取り込みなどを実現できることが不可欠となっているといえます。

これらの要件を満たす一つの選択肢として、クラウド・サービスの利用に期待が高まっており、採用事例が増えています。クラウド・サービスを利用した場合に、医療機関などに求められる安全基準をどのように評価し満たすことができるのかを考える際に、「3省4ガイドライン」および、同ガイドラインに対する評価レポートである「医療機関向け『IBM Cloud IaaS』対応セキュリティー・リファレンス」[8]を活用できます。

4-2-2. 医療情報システムにおけるセキュリティー基準（3省4ガイドライン）

厚生労働省は、医療情報の機微性の高さを踏まえて、医療情報システムの安全管理およびe-文書法への適切な対応を行うために必要となる対策を技術的・運用管理上の観点から示した「医療情報システムの安全管理に関するガイドライン」[9]を発行しています。同ガイドラインをベースに、総務省はASP・SaaS事業者の観点、経済産業省は医療情報を受託管理する情報処理事業者の観点で、補強するガイドラインを発行しています[10][11]。これらの3省が発行した4つのガイドラインの総称が3省4ガイドラインです（**表3**）。

4-2-3. IBM Cloudは3省4ガイドラインに適合可能

3省4ガイドラインには計400以上の要求事項があり、個別に評価を行うことは大変な労力を必要とします。そこ

表3. 3省4ガイドラインの説明

ガイドライン	省庁	ガイドラインの目的
医療情報システムの安全管理に関するガイドライン 第5版	厚生労働省	医療機関等における電子的な医療情報の取り扱いに係る責任者を対象とし、医療情報システムの安全管理やe-文書法への適切な対応を行うため、技術的および運用管理上の観点から所要の対策を示したもの。[9]
ASP・SaaSにおける情報セキュリティ対策ガイドライン※	総務省	ASP・SaaSサービスの利用が企業等の生産性向上と健全な基盤となるよう、ASP・SaaS 事業者における情報セキュリティー対策の促進に資するため、ASP・SaaS事業者が実施すべき情報セキュリティー対策を取りまとめたもの。[10]
ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン 第1.1版	総務省	ASP・SaaS事業者が医療情報を取り扱う際に求められる責任等、ASP・SaaS事業者への要求事項等、合意形成の考え方を示すこと。これを通じて、医療情報がASP・SaaSによって適正かつ安全に利用され、医療情報におけるASP・SaaSの利用の適切な促進を図ること。[11]
医療情報を受託管理する情報処理事業者向けガイドライン 第2版	経済産業省	「医療情報の外部委託」という事業特有の課題に配慮し、この分野において情報セキュリティー・マネジメントシステムを実装する上でのガイドラインを示すこと。[12]

※2018年7月31日に「クラウドサービス提供における情報セキュリティ対策ガイドライン（第2版）」に統合

で、主に医療機関・SI事業者等が医療情報システムをIBM Cloud インフラストラクチャー（以下、IBM Cloud IaaS）上に構築・利用する場合を想定して、株式会社三菱総合研究所による適合可否の調査および評価を行った結果を公開しています[13]。評価の結果、IBM Cloud IaaSに保管するお客様データへのアクセス権をIBMが持たないことなどから、IBM Cloud IaaSの管理範囲についてはすべて適合可能であり、お客様責務にて実施いただく項目への対応を行うことで、3省4ガイドラインに準拠できることが確認されています。

IBM Watson APIやデータ分析ソリューションなどのIBM Cloud経由で利用可能なサービスを組み合わせることにより、医療サービスにおける先進的な取り組みを支援するITプラットフォームとしての活用が、今後ますます見込まれています。

5. GDPRへの対応

2018年5月25日、EUの個人情報保護法であるGDPR（General Data Protection Regulation：一般データ保護規則）が施行されました。これは従来のEUデータ保護指令をより厳格に法制化したものです。世界各国の個人情報に関する法規制は、1980年OECD（Organization for Economic Co-operation and Development：経済協力開発機構）が制定した「プライバシー保護と個人データの国際流通についてのガイドライン」のOECD8原則を基礎としています。GDPRではさらに、自国の個人情報の他国への持ち出しを原則禁止し、違反に対する高額な罰則（年間売上の4%、または2,000万ユーロ（約26億円）のいずれか高い方）を課すなど、概して厳しい内容になっています。欧州委員会により適切な個人情報保護制度を有していると認定されていない国への情報移転に際しては、企業は拘束的企業準則（Binding Corporate Rules）の策定、標準契約条項（Standard Contract Clauses）の締結といった要件を満たす必要があります。日本はEUと実質的な合意をし、公式な認定に向けて準備中です[14]。

IBM Cloudは、GDPRへの対応をいち早く表明しています。現在IaaSおよびPaaSの24のサービスについてクラウド・プロバイダーが利用者のGDPR対応に向けて順守すべき行動規範（EU Data Protection Code of Conduct for Cloud Service Providers）に署名済みです[15]。お客様はこれらのクラウド・サービスやデータ・ストレージ、データ処理ソリューションを使用してGDPR対応を準備することで、データの透明性と制御能力の向上、効率化など迅速な革新が実現できます。またIBMは、お客様のGDPR対応を支援する5段階のGDPR

図3. IBMのGDPRフレームワーク

フレームワークにより（**図3**）、各段階を支援するサービスやソリューションを提供しています[16]。お客様は、これらのサービスを活用することでGDPRに対応したシステムの展開をスムーズに行えます。

6. おわりに

ビジネスの成功を実現させるための手段の一つとしてのクラウドは、自社のコンプライアンスにどう対応できるかといった仕組みの透明性が重要視されます。3省4ガイドライン、FISCやGDPRの施行など、ITを取り巻くコンプライアンスが時々刻々と更新される中、クラウド・ベンダーが公開しているコンプライアンス情報を活用することで、スピード感をもってシステム全体としての対応の評価が可能です。

[参考文献]
[1] セキュリティ関連NIST文書, 情報処理推進機構, https://www.ipa.go.jp/security/publications/nist/
[2] Tier Classification System, Uptime Institute, https://uptimeinstitute.com/tiers
[3] 日本データセンター協会制定データセンター・ファシリティ・スタンダードの概要, 日本データセンター協会, http://www.jdcc.or.jp/pdf/facility.pdf
[4] Compliance on the IBM Cloud, IBM, https://www.ibm.com/cloud/compliance
[5] FISC, 金融機関等コンピュータシステムの安全対策基準・解説書（第9版）, https://www.fisc.or.jp/guideline/updata/
[6] IBM Cloudのリスク調査結果, https://www.ibm.com/cloud-computing/jp/ja/softlayer_fisc.html
[7] 金融機関等コンピュータシステムの安全対策基準第8版追補改定　IBM Bluemixにおける対応状況, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=KUI12357JPJA
[8] 株式会社三菱総合研究所：医療機関向けクラウド・サービス対応セキュリティー・リファレンス, https://www.mri.co.jp/service/201602_021630.html
[9] 厚生労働省：医療情報システムの安全管理に関するガイドライン　第5版, 2017年5月, https://www.mhlw.go.jp/stf/shingi2/0000166275.html
[10] 総務省：ASP・SaaSにおける情報セキュリティー対策ガイドライン, 2008年1月30日
[11] 総務省：ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン 第1.1版, 2010年12月
[12] 経産省：医療情報を受託管理する情報処理事業者向けガイドライン 第2版, 2012年10月, http://www.meti.go.jp/policy/it_policy/privacy/kojin_gadelane.html
[13] IBM Cloudについて「医療業界向け3省4ガイドライン」への対応を確認 日本での医療・ヘルスケア業界向けクラウド・サービスを加速 https://www-03.ibm.com/press/jp/ja/pressrelease/54200.wss
[14] 日本経済新聞：個人データ相互移転 日欧が合意 今秋にも枠組み発効, 2018/6/1, https://www.nikkei.com/article/DGKKZO31205640R30C18A5MM8000/
[15] IBM：IBM and the EU Data Protection Code of Conduct for Cloud Service Providers, https://www.ibm.com/privacy/details/us/en/scope_europe.html
[16] IBM：「IBMが示すGDPR対応への道」, https://www.ibm.com/account/reg/jp-ja/signup?formid=urx-21220

日本アイ・ビー・エム株式会社
IBMクラウド事業本部
Watson & Cloud Platform テクニカルセールス
シニア・アーキテクト

安田 智有
Tomoari Yasuda

1999年日本IBM入社。音楽配信アプリのプログラマーを経て、Grid Computing、分散コンピューティングや可視化のスペシャリストとして活動。2010年からアーキテクトに従事。2015年からクラウドのエンジニア集団を率いるマネージメント・チームに合流。

百瀬 孝三
Kohzo Momose

1990年日本IBM入社。CISSP（Certified Information Systems Security Professional）ホルダー。ネットワーク&セキュリティースペシャリストを経て、2014年よりクラウド・テクニカル・セールスとしてクラウド全般のソリューショニングを担当。

日本アイ・ビー・エム株式会社
グローバル・テクノロジー・サービス事業部
IBM Cloud Solutioning Center - East
アドバイザリー・アーキテクト

上田 夏奈江
Kanae Ueda

日本IBM入社後、金融業界のお客様におけるアウトソーシング・サービスの運用および提案活動を行う。クラウド・サービスの立ち上げを機に、2011年から業界横断的にクラウド・サービスを活用したITシステムの提案およびソリューショニングを担当。