（別紙）

2024 年 1 月

クラウドサービス[1]利用において必要な管理項目と具体的な取組事例[2、3]

[1] 以下、クラウドと略す。

[2] 本資料は金融機関に一律の取り組みを促すことを目的としたものではない。例えば、システムの重要度によって、求められる取り組みには違いが生じ得るほか、クラウド事業者の方針によっては、取り組みが現実的に難しいケースも考えられる。金融機関においては、それぞれの業務内容やシステムの重要度等を踏まえ、リスクベースで対応することを期待している。

[3] 本資料は可能な限りクラウドのサービス分類（IaaS、PaaS 等）によらず汎用的に利用できるように整理している。実際には、サービス分類により金融機関とクラウド事業者が運用・管理する範囲は異なるが、クラウド事業者が運用・管理する範囲であっても、金融業務のベースとなる情報およびその情報を取り扱うプロセスの管理に関しては金融機関側に責務が生じることから、委託先管理の枠組みの下で必要な管理水準を確保する必要がある。

目次

1. クラウドの導入

管理項目	取組事例	（参考）関連する規格[4]			
		NIST	ISO	FISC	ISMAP
1.1 導入の前提事項					
➢ クラウド利用に関する適切な検討・管理体制を整備すること	○　クラウド利用に関する方針やクラウド導入に伴い業務運営面やリスク管理面で必要となる対応事項等について、経営会議や取締役会の関与の下、定めている ○　システム関連部署に加え、リスク管理部署や契約部署等、広く関係者を含めた横断的な組織を構築し、クラウド利用に伴うリスク管理や業務面の課題解決について検討している	144-9.1	6.1	統 20	―
➢ 機密性、可用性、経済合理性を適切に判断すること	○　クラウドへの移行可否の検討に際しては、取り扱う情報に応じた機密性、対象業務に応じた可用性を満たしているかチェックリストで確認している ○　選択するクラウドのサービスにより経費が大きく変動することを踏まえ、コストシミュレーションにより経費を比較し、最適なサービスを選択している	144-5.2	15.1.1 15.2	統 20	―
➢ クラウド事業者を適切に選定すること	○　クラウド事業者の選定にあたっては、経営体力・収益力、サービス品質、セキュリティ管理体制（アクセス管理、環境分離、認証強度、脆弱性対応、伝送データの漏洩防止等）、サポート体制、サービス利用終了時の対応（データの消去方法、消去可能な範囲等）、委託先の管理体制、反社会的勢力の排除の扱い等を確認している ○　クラウド事業者の選定にあたっては、オンプレミスからの移行時のツール提供や情報提供などのサポート力を重視している ○　クラウド事業者の選定時に、金融機関が直接的に確認できない事項については、第三者保証による報告書等により確認している。	144-5.2	4.3 18.1.1	統 20 統 24	―

[4] 「（参考）関連する規格」で示す規格は以下のとおり。
NIST：NIST Special Publication 800-144 および 800-146、ISO：ISO/IEC27017、FISC：安全対策基準（第 11 版）、ISMAP：政府情報システムのためのセキュリティ評価制度管理基準

管理項目	取組事例	（参考）関連する規格[4]			
		NIST	ISO	FISC	ISMAP
1.2 契約締結時の留意事項					
➢ 契約、SLA の適切性を確保すること	○　クラウド上のデータの所有権、データ保護、サービスの変更・停止、課金、業務委託、内部・外部監査結果の提示、紛争時の解決手段、準拠法、監査権、契約解除について、契約上の扱いを確認している ○　SLA で、品質（稼働率、性能等）、料金、サポート期間、サービス品質を満たさなかった場合の扱い等を確認している ○　サービス停止等が生じた場合におけるクラウド事業者の賠償の扱いを確認し、想定される損害に見合わない場合は、保険等によりリスクを移転している ○　重要業務については、クラウド事業者がサービスを提供できなくなった場合に、他のクラウド事業者への移管等を支援する項目を契約に含めている	144-5.3 146-8.3.2	13.2.4 18.1.1	統 21 統 24	15.1.1 18.1
➢ 必要に応じ追加的な取り決めを行っておくこと	○　サービス停止の影響範囲を整理した上で、メンテナンス時の事前報告および停止時間帯の調整に関する項目を契約等に補足している ○　業務に影響を与える可能性のあるクラウドの仕様、機能、設定の変更は事前に金融機関に報告されるように取り決めている ○　クラウド事業者が取得するログの範囲および保存期間を確認した上で、障害やセキュリティ侵害発生時のログ提供に関する覚書を取り交わしている	144-5.3	18.1.1	統 21 統 24	15.1.1 18.1
➢ 必要に応じ海外を含めた法規制の確認を行うこと	○　海外拠点でクラウドを利用する場合は、当該国のクラウドに関する規制を確認している	144-4.2 144-5.2	18.1	統 21 統 24	15.1.1.16.B 18.1

管理項目	取組事例	（参考）関連する規格[4]			
		NIST	ISO	FISC	ISMAP
1.3 金融機関内部の管理基準の策定					
➢ セキュリティ規格等に則した管理基準を策定すること	○　クラウドのセキュリティ規格やクラウド事業者が纏めた運用やセキュリティに関する事例集等を参考に管理基準を定めている （セキュリティ規格の例） FISC 安全対策基準および同監査基準、ISMAP、ISO/IEC27017・27018・27036、NIST SP800-144・SP800-146、FedRAMP、CSA CCM、ENISA クラウドセキュリティガイドライン、CIS ベンチマーク、JASA クラウドセキュリティ推進協議会 CS ゴールドマーク	144-4.1	5.1.1 6.1.1 CLD-6.3.1	統 1	—
➢ 適時適切に管理基準の見直しを行うこと	○　以下の方法でセキュリティ規格の変更に合わせ管理基準を見直している ①セキュリティ規格と管理基準の対応関係を記録として残し、セキュリティ規格の改訂に合わせて管理基準を見直せるようにしている ②外部監査やセキュリティベンダーも活用してセキュリティ規格の変更点を確認している ○　クラウド事業者が提供する SOC2 レポートやセキュリティに関する報告書等により、サービスや技術の変化を確認した上で、管理基準の見直しを検討している ○　クラウドの障害やセキュリティ侵害の原因分析を定期的に行い、管理基準の課題を洗い出し、改善に繋げている	144-4.1	12.1.2	統 1	—
➢ 管理対象から外れるクラウドの利用を防ぐこと	○　以下の方法を用い、管理対象から外れるクラウドの利用を防止している ①クラウドの利用状況を可視化する外部サービスの活用 ②クラウド事業者から提出される利用サービス一覧の検証 ③クラウド事業者との契約状況を契約部署に照会	144-4.1	6.1.1 CLD-6.3.1	—	—

2. セキュリティ管理

管理項目	取組事例	（参考）関連する規格			
		NIST	ISO	FISC	ISMAP
2.1 責任共有モデルを踏まえたクラウド事業者との連携					
➢ 金融機関とクラウド事業者が運用・管理する範囲を適時適切に確認していること	○　サービス導入前に、クラウドの分類（IaaS、PaaS 等）を考慮したうえで、クラウド事業者が金融機関に開示するサービス内容やセキュリティに関する報告書および各サービスの SLA 等を元に、金融機関とクラウド事業者が運用・管理する範囲を確認している ○　サービス導入後、機能追加等に伴いクラウド事業者が運用・管理する範囲が変化していないか定期的に確認している ○　コンテナのベース OS、標準ライブラリ等において、運用・管理する主体に不明確なものが生じた場合は、その都度、クラウド事業者に確認している	144- 4.1 146- 付録 A	6.1.1 CLD- 6.3.1	統 24	6.1.1. 13.PB
➢ 障害発生等に備えてクラウド事業者と連携していること	○　障害やセキュリティ侵害発生時のクラウド事業者による通知の仕組みを踏まえて、金融機関内の連絡体制を構築している ○　クラウド事業者との契約において、障害やセキュリティ侵害が発生した場合の金融機関への通知方法等を事前に定めている ○　障害やセキュリティ侵害発生時の対応策や復旧策について、クラウド事業者と利用者側の責任範囲を確認している ○　セキュリティ侵害時にオンプレミスとは異なるフォレンジック手法が必要となることを踏まえ、クラウド事業者とフォレンジック手法について予め合意している ○　クラウド事業者側が取得しているバックアップについて、その対象範囲や取得タイミング、保管する世代数、保持期間やセキュリティ侵害対策等を確認している ○　金融機関とクラウド事業者のシステム時刻が共に正確になっていることを確認している	144- 5.2 146- 8.2 146- 8.4.4 146- 付録 A	6.1.1	統 21 統 23 実 19 実 39	4.9.2

管理項目	取組事例	（参考）関連する規格			
		NIST	ISO	FISC	ISMAP
2.2 外部ネットワークからの不正アクセス防止					
➢ 外部との通信手段のセキュリティを確保すること	○ 機密性が求められるデータ通信については、専用回線、VPN、SDP 等を用いている ○ API を通じて外部アプリケーションサービス事業者と通信する場合は、認証手順が適切に設定されていることを確認している	144-4.4 146-4.2	13	実 4 実 7	13
➢ 外部との通信経路を制限しクラウドにアクセスする端末のセキュリティを確保すること	○ ファイアウォールや不要な通信ポートの閉塞によりアクセス経路を制限している ○ 管理インターフェースへのアクセスを認める IP アドレスや端末を限定している ○ クラウドにアクセスする端末は、ウイルス対策、データの書出防止、不正利用防止機能（ログイン管理、自動ログオフ等）により、セキュリティを確保している	144-4.4 146-8.5.5	12.2 13	実 14 実 15 実 35	9.1.2
➢ 外部からの異常なアクセスを検知・防御する対策を行っていること	○ 想定外の経路からのアクセスがないか、定期的にログを検証している ○ 外部アプリケーションサービス事業者との通信に異常がないことを、呼出回数、遅延、エラー等の指標を用い監視している ○ WAF によってウェブアプリケーションの脆弱性を悪用した攻撃等を防止している	144-4.4 146-8.2.1	13.1.1	実 14 実 16	13
2.3 金融機関内部も含めた不適切なアクセス等の防止					
➢ アクセス権限を管理すること	○ 管理インターフェース、仮想マシン、コンテナ環境およびデータへのアクセス権は最小権限の原則に沿って付与し、不要になった ID は速やかに削除するなど定期的に棚卸しする体制を整備している ○ 管理インターフェースについては、アクセス時間を制限するツール（Just in Time 方式）や予め登録した作業内容と操作状況を比較し不正利用があった場合に検知するサービスを導入している	146-9.3	9.2 9.4.1	統 24 実 25 実 27	9.2

管理項目	取組事例	（参考）関連する規格			
		NIST	ISO	FISC	ISMAP
	○　重要業務については、アクセス権限に関する仕様変更について、クラウド事業者から事前に変更内容が通知されることを確認している ○　アクセス権限の設定変更や仕様変更が生じた場合は、必要に応じて専門家によるシステム監査や誤設定の自動検知等の診断サービスを活用しながら、設定内容の妥当性を確認している				
➢ 正当な権限者以外による利用を防止すること	○　多要素認証により不正利用のリスクを低減している ○　クラウド内に仮想的な金融機関専用の領域を構築することで、他のクラウド利用者による利用を防止している	144-4.5	9.4	実 9	9.4
➢ ログの検証等により不正利用を検知すること	○　アクセスログを定期的に検証することにより不正利用の有無を確認している ○　管理インターフェースの操作ログをリアルタイムでモニタリングし、操作ログや操作画面の録画等により操作証跡を取得している	144-4.9 146-9.1	12.4	実 10	12.4
2.4 データの保護					
➢ データの所在を把握し暗号化等を行っていること	○　コンテナに保持するものも含めて、データのリージョン単位の所在および求められる機密性やアクセス制御の状況を台帳等により整理し定期的に点検している ○　高い機密性が求められるデータは、適切な強度で暗号化し、暗号化鍵は生成、利用、廃棄までの一連のサイクルを管理している ○　暗号鍵へのアクセスについては、アクセス制限やアクセスログの保管・モニタリング等により、適切に管理している	144-4.7 146-8.1.4 146-8.5.2	8 10	実 3 実 4 統 24	8 10
2.5 セキュリティ対策の実効性確保					
➢ クラウドの特性を踏まえたサイバー攻撃対策を行っていること	○　金融 ISAC やクラウド事業者のサービス等を利用して、継続的にサイバー攻撃に関する情報やクラウド事業者が提供するサービスで利用しているハードウェア・OS・ソフトウェアの脆弱性情報を収集し対策を講じている ○　CSA が公開しているセキュリティ侵害事例の分析資料を用い、紹	144-4.4	12.6	統 4 統 5 統 24	12.6

管理項目	取組事例	（参考）関連する規格			
		NIST	ISO	FISC	ISMAP
	介されているセキュリティリスクに金融機関が対処出来ているか検証している				
➢ セキュリティ対策が機能していることを確認すること	○　定期的に脆弱性診断、ペネトレーションテスト、セキュリティベンダーによるアセスメント等を実施している ○　WAF 等のセキュリティツールをクラウド上で利用する場合は、金融機関に必要な設定が有効になっているかを確認している ○　セキュリティに関する設定変更を自動検知し、設定に問題が発見された場合は元に戻す仕組みを導入している ○　セキュリティ対策に影響を及ぼす不正操作が行われていないか、クラウド事業者のツール等を用いて監視している	144-2.1	12.6	統 5	12.6
2.6 クラウド利用に関するセキュリティ教育体制					
➢ クラウド固有のセキュリティリスクに関する教育体制を整備していること	○　クラウド固有のセキュリティリスク（設定ミス等による重要情報の漏洩、未承認のクラウドサービスの利用等）を抑制するため、役職員への教育体制を整備している	—	—	統 14	4.5.2

3. 可用性管理

管理項目	取組事例	（参考）関連する規格			
		NIST	ISO	FISC	ISMAP
3.1 クラウドに適した運用管理					
➢ ログを収集し適切にモニタリングすること	○　マネージドサービス、クラウド事業者のツール、サードパーティソフト等を活用し、クラウドの運用管理に必要なログを収集・モニタリングしている ○　クラウドだけでなくオンプレミスのログも一括して運用監視できる統合ログ管理ツールを用いている ○　クラウド事業者のログ出力のタイムゾーンを確認している	144-4.9	12.4	実 10	12.4

管理項目	取組事例	（参考）関連する規格			
		NIST	ISO	FISC	ISMAP
➢ サービス変更や廃止を早期に把握すること	○　定期的にサービス変更や廃止の案内を確認している ○　定期的にクラウド事業者と打合せを行うことで、サービス変更等の情報を早期に入手できるようにしている ○　クラウド事業者がサービスを廃止する可能性に備え、早期に事前連絡を受ける契約を締結している ○　重要業務については、マネージドサービスの活用やクラウド事業者と特別な契約を締結することにより、影響を与える可能性のあるサービスの仕様、機能、設定の変更を早期に把握し、迅速に対応できるようにしている	144-3.1 144-4.3	15.2.2	統 21	15.2.2
3.2 システム性能の確保					
➢ 業務に必要なシステム性能を把握すること	○　オンプレミスと同様、事務量、業務プロセス、システム構成を踏まえた机上試算を行い、クラウド上で必要となるシステム性能を把握している	144-4.4 144-5.3	12.1.3	実 47	12.1.3
➢ システムの使用率等のモニタリングを行うこと	○　クラウド事業者が提供するツール等を活用し、利用するコンピューター資源の使用率等を金融機関が一括監視している	144-4.3 144-5.3	12.1.3	実 47	12.1.3
➢ 適時適切にシステム性能を拡張すること	○　クラウドのサービス毎の拡張性や上限を把握し、必要なシステム性能が変化した場合には、適時適切に上限を引き上げている	—	12.1.3	実 47	12.1.3
3.3 可用性の高いシステム構成					
➢ 冗長性を確保したシステム構成等とすること	○　ゾーンやリージョンの組み合わせにより冗長性を確保することで、メンテナンスや障害によるサービス停止が生じにくいようにしている	—	17.2	実 73 実 74	17.2

4. レジリエンス

管理項目	取組事例	（参考）関連する規格			
		NIST	ISO	FISC	ISMAP
4.1 レジリエンスの確保					
➢ サービス停止を想定した対応手順を整備すること	○　クラウド事業者が提供する障害検知サービスを活用し、障害（セキュリティ侵害によるものを含む）を早期に発見・把握できる体制を整えている ○　業務の重要度や求められる可用性の水準に応じ、クラウド事業者との間で障害対応に関するサポートサービスを決めている ○　クラウド上に構築したシステムについて、クラウドのサービス停止に起因するシステム障害が発生した場合のシステムへの影響範囲の確認と復旧対応（再発防止策の策定などを含む）に関する役割分担を開発委託先との間で定めている ○　パイロット運用の段階で、クラウドサービスの障害発生傾向も踏まえて障害対応手順を整理しておくことで、本格利用に円滑に移行できるようにしている ○　クラウドサービスの障害発生傾向も踏まえ、金融機関で対応可能な障害対応手順を準備している ○　障害対応手順（バックアップデータからの復旧、バックアップシステムへの切替等）の訓練を定期的に行うことで、その実効性を確保している ○　重要業務については、クラウド事業者の委託先やクラウド事業者が利用する外部サービスが起因となって発生した障害の対応策について考慮されていることを確認している	144-4.8	15.1.1	統 24 実 24 実 70 実 71 実 72	—
➢ 災害等に備え重要業務を継続できる体制を整えていること	○　重要業務については、利用するクラウドのデータセンターが被災した場合を想定した業務継続計画を整備している ○　業務または組織の存続のために特に重要なデータについては、必要に応じて金融機関のデータセンターや別のクラウド事業者のクラ	144-4.8	17	実 73 実 74	17

管理項目	取組事例	（参考）関連する規格			
		NIST	ISO	FISC	ISMAP
	ウドにバックアップデータを保管するなどにより、重要業務を継続できるようにしている				

5. コスト管理

管理項目	取組事例	（参考）関連する規格			
		NIST	ISO	FISC	ISMAP
5.1 コスト構造の把握と抑制					
➢ クラウドのコスト構造を適切に把握していること	○　従量制の課金体系が多いことを踏まえ、事務量が変動した場合の影響をコストシミュレーションにより確認することで、経費が膨らむリスクを定期的に把握している ○　クラウドにかかる経費にアラートや上限を設定する等により想定外の経費の上振れ防止や早期発見ができるようにしている	144-4.1	12.1.3	―	―
➢ コスト抑制策を実施していること	○　事務量に応じたコンピューター資源（CPU やハードディスク等）の調整や、使用しないサービスの停止等によって、コストを抑制している ○　テスト環境は可用性の低い廉価なサービスを選択し、長期利用が見込まれるサービスは固定契約割引を活用するなど、利用形態に沿ったサービスを選択することでコストを抑制している	146-8.3	―	―	―

6. 開発体制・人材確保

管理項目	取組事例	（参考）関連する規格			
		NIST	ISO	FISC	ISMAP
6.1 クラウドに対応した開発体制					
➢ サービス仕様の変更等を把握していること	○　クラウド事業者が WEB 等で公開するサービスの仕様変更等の情報を能動的にモニタリングしている ○　利用するサービスと業務を紐づけることで、仕様変更等の影響確認および対応を円滑に行えるようにしている ○　サードパーティの買収等によりクラウドに組み込まれたサービスは、他のサービスと仕様が異なる場合があることから、改めて SLA やクラウド事業者のサービスに関する報告書等で確認している	144-5.3	12.1.2	統 24	12.1.2
➢ クラウドの特性を踏まえた開発手順を整備していること	○　クラウド事業者が公開している事例集等を活用しながら、開発の標準的な手順について、仮想化技術、拡張性、リージョン・ゾーン等のインフラ構成等を踏まえたものに見直している ○　クラウド関連の技術やサービスの変化の速さに対応するため、開発、テスト、リリースまでの一連の作業の自動化や運用と開発の一体化（DevOps）を進めている ○　開発の効率性向上やシステムの疎結合化による保守性向上等のためマイクロサービスを利用する場合には、構成の複雑化に伴うマイクロサービス間の通信の輻輳による性能低下、障害点の増加、運用の複雑化といったデメリットも踏まえたシステム設計を行っている	144-4.1 144-4.4	14.2	実 75	14.2
6.2 クラウド人材の確保					
➢ クラウドに精通した人材育成、確保を行っていること	○　以下の方策によりスキルアップ計画を策定し、クラウドの専門知識に精通した人材を育てている ①クラウド関連の資格取得、クラウド事業者が開催するイベントや研修を活用している ②IT ベンダーや外部コンサルタントから、クラウドの仮想化技術やリージョン・ゾーン等のインフラ構成等に精通した有識者の派遣	144-3.2 144-5.1	7.2.2	統 24	―

管理項目	取組事例	（参考）関連する規格			
		NIST	ISO	FISC	ISMAP
	を受けている ③既存システムの開発担当者に、クラウドに関する知識獲得を慫慂している ○　内部監査部門にもクラウドに関する技術や特有のリスク管理に関する情報を習得させている ○　外部のセミナーや講演等で、金融機関のクラウドに対する取り組みを紹介することで、クラウドに精通した人材の活躍の場があることをアピールしている				

7. 委託先管理

管理項目	取組事例	（参考）関連する規格			
		NIST	ISO	FISC	ISMAP
7.1 委託先の管理状況の把握					
➢ クラウド事業者の管理状況を把握すること	○　クラウド事業者の SOC2 レポート、監査報告書、サービスやセキュリティに関する報告書等を定期的に確認し、事業者のサービスの稼働実績、セキュリティ管理、運用管理、委託先の統制状況を把握している。課題がある場合は事業者に改善を働きかけている ○　クラウド事業者の SOC2 レポート等により、ハードウェア等の再利用や廃棄時の運用（データ消去の実施状況等）を確認している	144-4.3	15	統 21 統 23 監 1	15
➢ クラウド事業者のリスク管理体制を実地で確認できるようにすること	○　重要なセキュリティ侵害やシステム障害の発生に備え、統制対象クラウド拠点[5]を把握し、同拠点に対する監査権を確保するか、その代替として、詳細な報告書を求めることができるようにしている ○　金融庁検査や日銀考査等、監督当局からの協力要請に対応できるようにしている	144-5.2 144-5.3	12.7	統 21	4.9
➢ クラウド事業者の委託先（以下、再委託先）の管理状況を確認すること	○　クラウド事業者の再委託先選定基準や条件、再委託するサービスの範囲を確認している ○　再委託先のリストを入手し、不適切な再委託先がないか検証している ○　SOC2 レポート、監査報告書等により再委託先の管理状況を確認している	144-4.3	15.1.3	統 21 統 23	—
➢ クラウドを利用する委託先を適切に管理すること	○　重要業務の委託先に対する定期的な確認項目に、クラウド利用の有無を含めている ○　クラウドに関する重要な管理項目のチェックリストを作成し、これを用いて委託先のクラウドの管理状況を定期的に検証している	—	15.1.3	監 1	—

[5] FISC 安全対策基準で定める「統制対象クラウド拠点」のこと。クラウド事業者への統制上必要となるデータへのアクセスが可能となる情報処理拠点等、実質的な統制を行うにあたり対象となる事業拠点を指し、クラウド事業者の本社、営業所、データセンター、オペレーションセンター等様々な拠点が候補となる。

（参考）用語集

用語	概要
オンプレミス	利用者の施設にコンピューターや情報機器を設置し、利用者自身がコンピューターや情報機器を管理する形態のこと
仮想化技術、 仮想マシン	仮想化技術は、コンピューターのリソースを、物理的な構成にとらわれずに柔軟に分割、統合させる技術のこと。 仮想化技術により構成したコンピューターを仮想マシンという
管理インターフェース	仮想マシンの追加・削除、ユーザー管理、ネットワーク設定等、クラウドの設定を自由に操作できる管理機能のこと
クラウド	共有可能なコンピューターのリソースの集積に、必要に応じネットワーク経由でアクセスすることを可能としたモデルのこと
コンテナ	稼働中の OS 上で別の OS に対応するライブラリやアプリケーションを利用するために隔離した専用領域のこと
最小権限の原則	情報資産にアクセスする人間、プロセス、プログラム等には必要最小限の権限のみを付与する原則のこと
ゾーン	リージョン内におかれるデータセンターの集合体のこと。通常、1 リージョンに複数のゾーンが準備される
疎結合	システムの構成要素間の結びつきや互いの依存関係が弱く、システム変更の柔軟性・機動性が高い状態のこと
標準ライブラリ	繰り返し利用するプログラムの部品を集めて、ひとまとめにしたファイルのこと
フォレンジック	セキュリティ侵害等が発生した際に行う、証拠保全、データ解析、関連情報の抽出までの一連の行為のこと
ホワイトリスト	接続やサービス提供を認める先を事前に定め、他の先との接続やサービス提供を認めない方式、または許可した先の一覧のこと
マイクロサービス	ソフトウェアを機能毎に細分化したもの。細分化したマイクロサービスを組み合わせてシステム構築を行うことで、システム変更や拡張をしやすくできる
マネージドサービス	システムの運用・監視、障害対応、保守等を請け負うアウトソーシングサービスのこと
リージョン	クラウドを利用するときに指定する、クラウドのサービスが提供され、データが保管されるエリア・地域のこと
リソース	ネットワーク、サーバー、ストレージおよびアプリケーションサービスのこと
レジリエンス	障害、自然災害、テロ、サイバー攻撃等が発生しても重要業務を継続できる能力のこと
CIS ベンチマーク	米国の CIS(Center for Internet Security)が発行しているセキュリティの好事例が記載されたガイドライン
CSA CCM	米国の民間団体クラウドセキュリティアライアンスが公表しているクラウドセキュリティの管理規格のこと。 Cloud Security Alliance Cloud Control Matrix の略

DevOps	開発・運用のチームが一体となり、開発から運用の工程を自動的かつ迅速に進めることができる体制のこと。開発（Development）、運用（Operation）の、それぞれの頭文字の略
ENISA クラウドセキュリティガイドライン	欧州ネットワーク情報セキュリティ庁（ENISA）が 2009 年 11 月に発行したクラウドコンピューティングのセキュリティに関するガイドラインのこと
ISMAP	クラウドの導入円滑化の観点から、日本政府が定めた基準に基づいたセキュリティ対策を実施していることが確認されたクラウドをリストに登録する制度。Information system Security Management and Assessment Program の略
ISO/IEC27017,27018	ISO（国際標準化機構）が 2014～2015 年にかけて公表した、クラウド上で従来の情報セキュリティ規格を満たすためのガイドラインのこと
NIST SP800-144	産業技術等に関する規格の標準化を支援する米政府機関（NIST）が 2011 年に公表した、パブリッククラウドのセキュリティ等に関する課題と考慮すべき事項を整理したガイドラインのこと
NIST SP800-146	NIST が 2012 年に公表した、クラウドを技術面から整理し、情報技術に関する意思決定を行う層への推奨事項を示したガイドラインのこと
SDP	外部との接続において、認証を接続先とは別の仲立ちするコントローラーに行わせることでセキュリティを高める仕組みのこと。Software Defined Perimeter の略
SLA	サービスの提供側と利用側との間での、サービス内容・範囲・品質等に関する合意または合意文書のこと。Service Level Agreement の略
SOC2 レポート	業務受託企業のセキュリティや可用性等の内部統制状況を対象に、監査法人が外部監査の国際認証（Service Organization Control）に従って、その有効性を検証した結果の報告書
VPN	暗号化技術等を用いて構築した仮想的なプライベートネットワークのこと。Virtual Private Network の略
WAF	ウェブアプリケーションの脆弱性を悪用した攻撃等からウェブアプリケーションを保護するソフトウェア、またはハードウェアのこと。Web Application Firewall の略

以　上