資料１－１

パブリッククラウド利用に関する技術検討作業班の進め方

2025年7月28日
事　　務　　局

検討の経緯及び課題認識

経　緯

- 2022年7月～2023年2月、本委員会において、クラウドネイティブ化に対応した技術基準の適用範囲等について議論。
- 2023年9月、技術基準の適用対象となる電気通信設備の範囲に、仮想化されたコア機能の提供に係る他者設備を含めるよう**電気通信事業法施行規則等を改正**し、他者設備（クラウドサービスの提供に係る設備を含む）を利用する電気通信事業者が当該他者設備を管理できるよう、**管理規程を整理**。

課 題 認 識

- 電気通信事業者の中には他者クラウドサービスの活用にメリットを感じる者が存在する一方で、**通信の秘密の関係**から他社のクラウドサービス上でデータを扱うこと、**役務の安定的な提供**が可能であるか等の観点から、**クラウドの活用を躊躇したり不安を感じるなどの課題を感じる者もおり**、**その活用の進展の阻害要因**となっている。

  ≪課題となる事例≫
  - 実際に電気通信事業法による責務を負う電気通信事業者と直接的にはその責務を負わないクラウド事業者との立場の違いから、利用契約の各種条件を巡って、締結に向けた調整が円滑に進まない場合がある（情報開示の範囲やオンサイトへの立入検査等）。
  - クラウド事業者側の障害を起因とし電気通信役務に事故が発生した場合、その復旧過程でクラウド事業者から適切かつ十分な支援や情報開示がなく、結果、社会インフラサービスである電気通信役務や、その利用者に不便が生じた例がある。
  - クラウド事業者に通信に関するデータを委ねる場合、通信の秘密の確保について、契約書等の書面で担保されているのみであり、具体的にどのような仕組みで担保されているのか不透明である場合がある。

- 社会インフラサービスである**電気通信役務の利用者への適切な提供の確保**に向け、「役務の安定的な提供」及び「通信の秘密」を念頭に置き、**電気通信事業者とクラウド事業者との協力や技術基準等の在り方について検討**を行うべきではないか。

技術基準として確保が求められる事項

- 電気通信設備の損壊又は故障により、電気通信役務の提供に著しい支障を及ぼさないようにすること
- 電気通信役務の品質の適正性の確保
- 通信の秘密の確保
- 他の電気通信事業者の接続する電気通信設備との責任の分界が明確であるようにすること
- 利用者又は他の電気通信事業者の接続する電気通信設備を損傷し、又はその機能に障害を与えないようにすること

検討の視座及び想定する課題設定

検討に際しての視座

- 社会インフラの一つである電気通信において、電気通信事業者には**電気通信事業法が求める規律に対する責務**のほか、利用者目線からも**社会経済活動に必須のインフラサービス提供者としての社会的責務**を負っている。
- 電気通信分野においてクラウド事業者の果たす役割は大きく、今後更に大きくなると見込まれる中においても、**国民に対し通信サービスの適切な提供を達成するためには、双方の連携が必要不可欠**。その際、**片方のみが不合理に責務を負うことにならないよう**に、また、**障害発生時には、利用者目線で、双方に連携**しながら対応することが望ましい点にも留意。
- 本分野における**クラウドの活用の動きを阻害させない**ようにする点や、電気通信事業が各分野を横断的に支える位置づけであることと同様、社会全体でクラウドサービスの利用が進めば、**クラウド事業者は実質的に社会インフラを支えるコアインフラ事業者の役目を担うこととなる**可能性や、あらゆる産業のインフラである**通信サービスが他社に依存**することにも留意。
- 類似の他分野における整理事例を踏まえつつも、**電気通信分野における特有の事情のあぶり出し**も重要。

想定する検討課題

- 社会経済活動に必要不可欠な通信サービスを国民に対して適切に提供できる環境を確保する観点から、電気通信事業者とクラウド事業者との関係の在り方を踏まえ、将来の制度見直しの根拠となる考え方を検討・整理。
- 想定される検討課題は、以下のとおり。

1　電気通信事業者が他者クラウドを利用する際に想定しておくべきリスク

- *他分野とも共通する事項のほか、電気通信分野特有の事情としての事項とは*
- *通信の秘密を念頭に、通信に関する信頼の起点及び安全性の担保方法の在り方とは*

2　上記リスクに対し、電気通信事業者とクラウド事業者とで満たすべき条件の在り方

- *電気通信事業者とクラウド事業者の各々の立場での役割及び責任の分担とは*

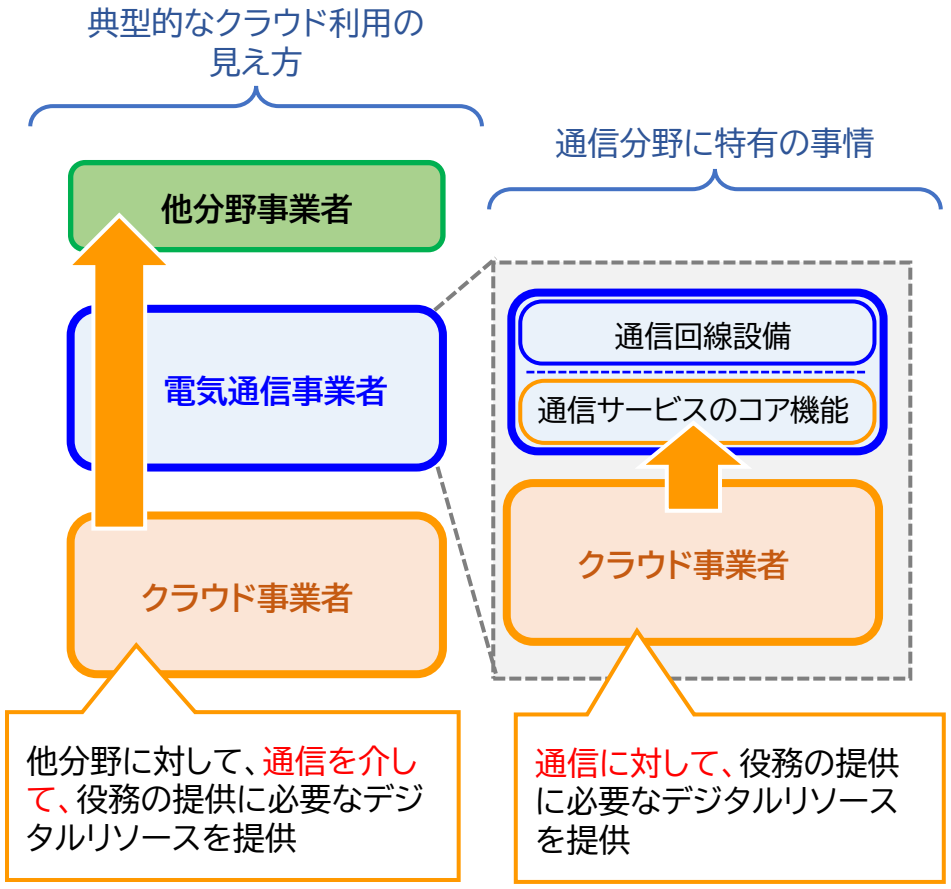
3　電気通信事業者が他者クラウドを利用する際の技術基準の在り方

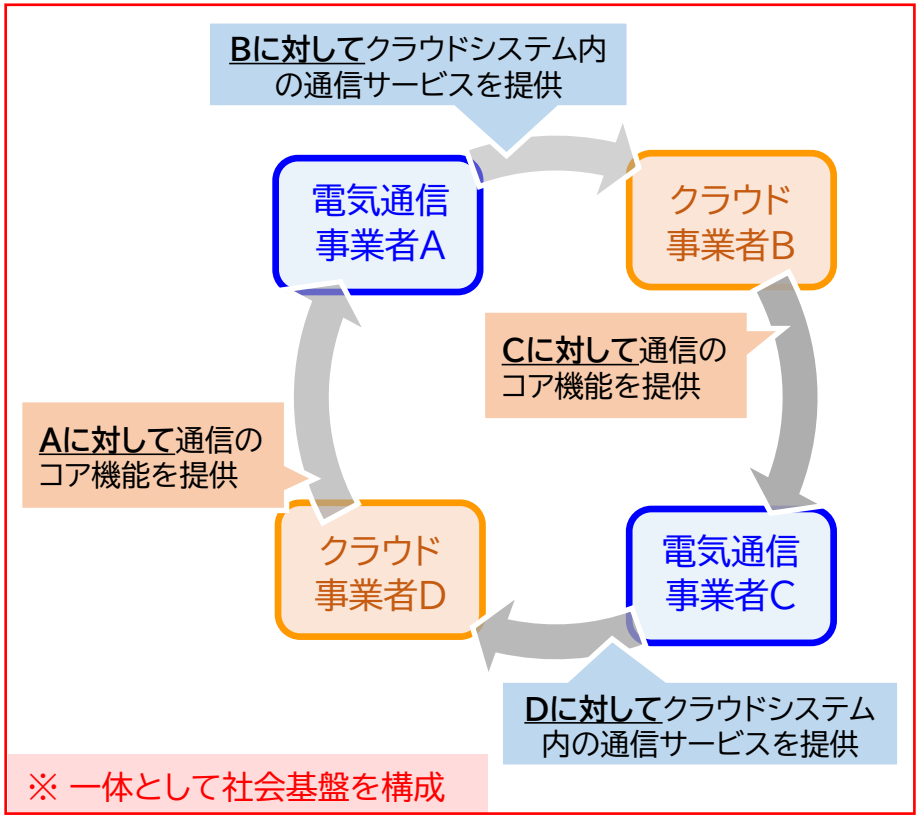
4　その他

電通通信事業者とパブリッククラウド事業者との関係

○電気通信事業者が、特にコア機能提供に係りクラウドサービス利用する際の特有の状況として、以下の点が想定される。

- ✓ **通信分野特有のリスクの有無の考慮**：クラウドサービス利用に不可欠な通信を担う側面とクラウドサービスの一利用者の側面の両面が存在する
- ✓ **サービスサプライチェーンや相互依存リスクの考慮**： サービスが多層的に相互に依存している場合がある
- ✓ **通信事業者とクラウド事業者の関係の在り方**： 電気通信事業者から見たクラウド事業者の立場やその関係（SIerや設備ベンダーのような立場か、通信機能を提供する通信事業者的な立場に当たるのか）





※サービスサプライチェーン上のどこかに支障が生ずると、関係するサービスに支障が連鎖するおそれが懸念

本日の作業班第1回について

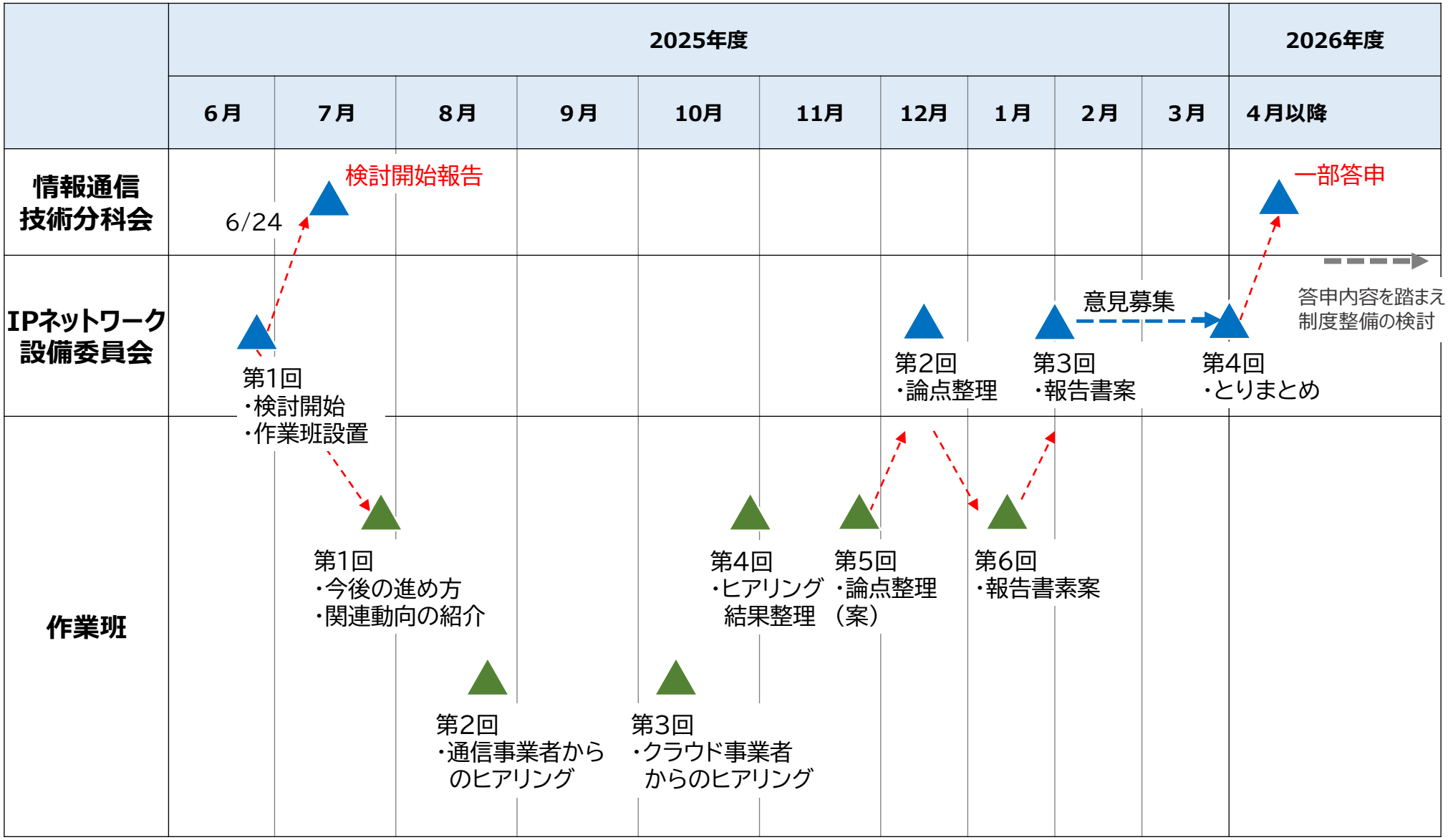
他者設備であるクラウドを利用することにあたっての留意事項の例

通信の秘密も含め、通信に関する安全・信頼性の担保方法の在り方を検討すべく、金融分野等の取組を参考にし、留意事項の例を導出

＼ 本日 ／

	留意事項の例	作業班第1回
データ保護	● クラウド事業者は、電気通信事業者が取り扱う通信に係るデータに技術上アクセスできるのではないか ● クラウド上で電気通信事業者が取り扱う通信に係るデータを蓄積、通信及び計算する際、暗号化された安全な空間になっているのか ● 電気通信事業者が利用するクラウドのオンサイトやシステムについて、第三者がアクセスできない形になっているのか　等	導入部として、関連する動向を紹介 **富士通株式会社より、データ保護に係る技術をご紹介**
管理体制	● クラウドに障害が発生した場合でも、そのデータの物理的な所在・状態などの詳細を電気通信事業者は把握できるのか ● クラウドに障害が発生した場合のほか、、クラウド上の機器やソフトウェアの脆弱性が判明したりした場合、必要十分な情報をクラウド事業者から情報開示がされるのか ● 利用するクラウドに重大な障害が発生し役務の提供に支障が発生した場合、電気通信事業者はクラウドに立入監査を行うことはできるのか　等	**デジタル庁より、政府が活用するクラウド環境をご紹介（非公開）**

今後のスケジュール（想定）



ヒアリング方針(案)

ヒアリング① 通信事業者からのヒアリング

固定系キャリア	● NTT東日本株式会社 ● NTT西日本株式会社
移動系キャリア	● 株式会社NTTドコモ ● KDDI株式会社 ● ソフトバンク株式会社 ● 楽天モバイル株式会社 ● 株式会社インターネットイニシアティブ

ヒアリング項目

- コア機能でのクラウド活用に係るニーズ（現時点、将来構想含む）
- クラウドを利用する場合に想定されるメリットや、課題及び留意事項等
- 上記課題や留意事項等の対応の在り方
- 制度整備を行う場合の要望 等

ヒアリング② クラウド事業者からのヒアリング

- グーグル・クラウド・ジャパン合同会社
- アマゾン ウェブ サービス ジャパン合同会社
- 日本マイクロソフト株式会
- 富士通株式会社
- さくらインターネット株式会社

ヒアリング項目

- クラウド利用者情報の保全、信頼の起点、責任共有の考え方と現状
- 平常時／障害発生時における利用者への情報提供の考え方と現状
- 制度整備を行う場合の要望 等

「パブリッククラウド利用に関する技術検討作業班」の検討体制

（令和7年7月時点）

氏名		主要現職
主任	内田　真人 ※	早稲田大学　理工学術院　教授
主任代理	田中　絵麻 ※	明治大学　国際日本学部　専任准教授
	宮田　純子 ※	東京科学大学　工学院情報通信系　准教授
	矢入　郁子 ※	上智大学　理工学部　情報理工学科　教授
	長谷川　剛	東北大学　電気通信研究所　情報通信基盤研究部門　教授
	堀越　　功	株式会社日経BP　日経ビジネスLIVE編集長
	吉田　　浩	国立情報学研究所　クラウド基盤研究開発センター　特任教授

※　IPネットワーク設備委員会メンバー

＜オブザーバー＞

固定系キャリア	● NTT東日本株式会社	● NTT西日本株式会社
移動系キャリア	● 株式会社NTTドコモ ● KDDI株式会社 ● ソフトバンク株式会社	● 楽天モバイル株式会社 ● 株式会社インターネットイニシアティブ
クラウド事業者	● グーグル・クラウド・ジャパン合同会社 ● アマゾン ウェブ サービス ジャパン合同会社 ● 日本マイクロソフト株式会社	● 富士通株式会社 ● さくらインターネット株式会社
ベンダー	● 日本電気株式会社 ● エリクソン・ジャパン株式会社	● ノキアソリューションズ＆ネットワークス合同会社
業界団体	● 日本クラウド産業協会	● 電気通信事業者協会

参　　考　　資　　料
（クラウドの関連動向）

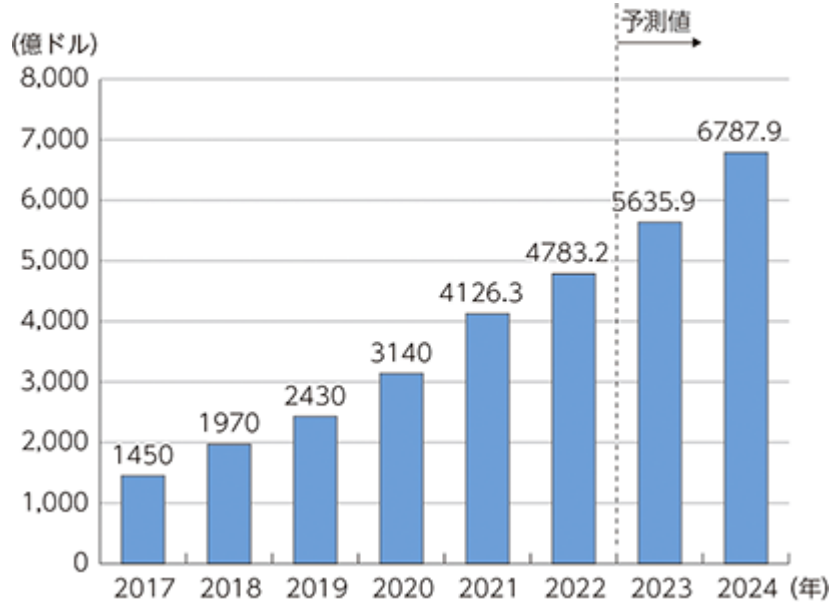
パブリッククラウドシステムを利用する際に想定されるメリデメ

メリット	デメリット
	経営視点の事項
1. 初期コストの削減 ・ハードウェア導入コストを大きく抑えられる。	**1. ランニングコストの増大** ・長期間・大規模に利用するとコストが高となる可能性。 ・突然の値上げや、外資系の場合は為替リスクが存在。
2. スケーラビリティ(拡張性) ・必要に応じてマシンリソースを柔軟に増減できる。	**2. カスタマイズ性の制限** ・提供サービスが利用者に応じてカスタマイズされない場合が多い。 ・クラウド事業者の都合でシステム更改が行われる場合がある。
3. 運用・保守の負担軽減 ・システムの運用・保守コスト(特に人的リソース)の軽減が期待される。	**3. 基盤システムに係る技術者やスキルの喪失** ・自社内での人材や技術が失われる(必要不可欠な部分が他者依存)。
4. 可用性・信頼性の向上 ・多くのクラウド事業者は高い可用性を保証しており、大規模な障害が発生しにくい。また、その復旧も比較的迅速に行われる。	**4. (クラウド)ベンダーロックインのリスク** ・他のクラウドシステムへの移行が難しくなるおそれがある。
	規律視点の事項
	5 通信環境に依存 ・クラウドシステムへの通信に障害が発生すると業務に支障をきたす。
5. セキュリティ対策 ・自社で対策するよりも最新かつ高レベルな保護が期待できる場合がある。	**6. セキュリティリスクの共有** ・クラウド事業者のセキュリティインシデントが自社にも影響する可能性がある。
	7.障害発生時の対応 ・利用者自身の努力では何もできない。 ・必要十分な情報提供を期待できない場合がある。
	8. 管理主権 ・データが保存場所が不明瞭となる。 ・クラウド上で扱うデータに対するクラウド事業者の関与の疑念が拭えない。

(事務局作成)

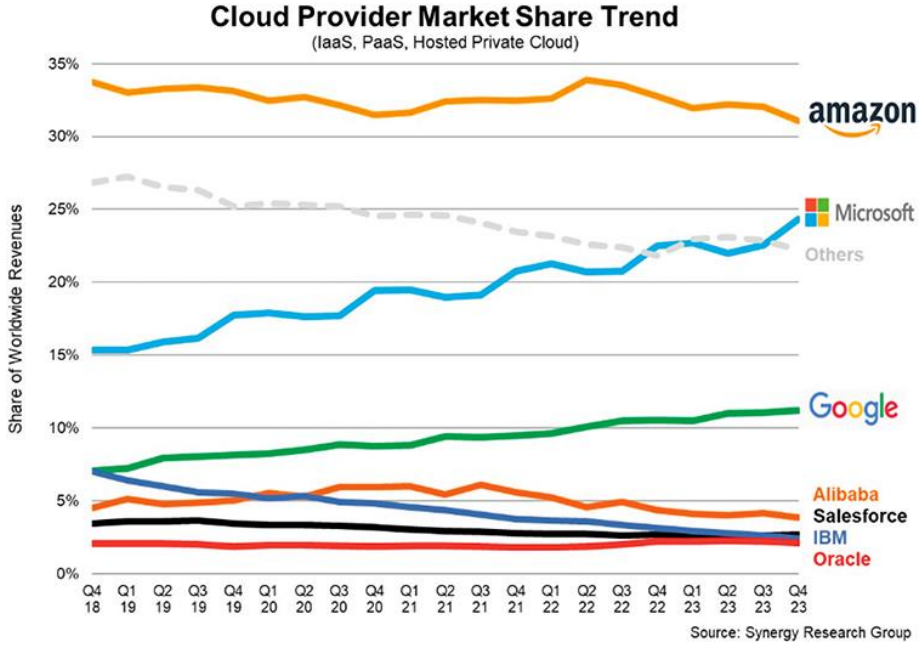
パブリッククラウドの市場動向

世界のパブリッククラウドサービス市場規模(支出高)の推移及び予測



(出典)ガートナー(Statistaより引用)

世界のクラウドインフラサービス市場のシェアの推移

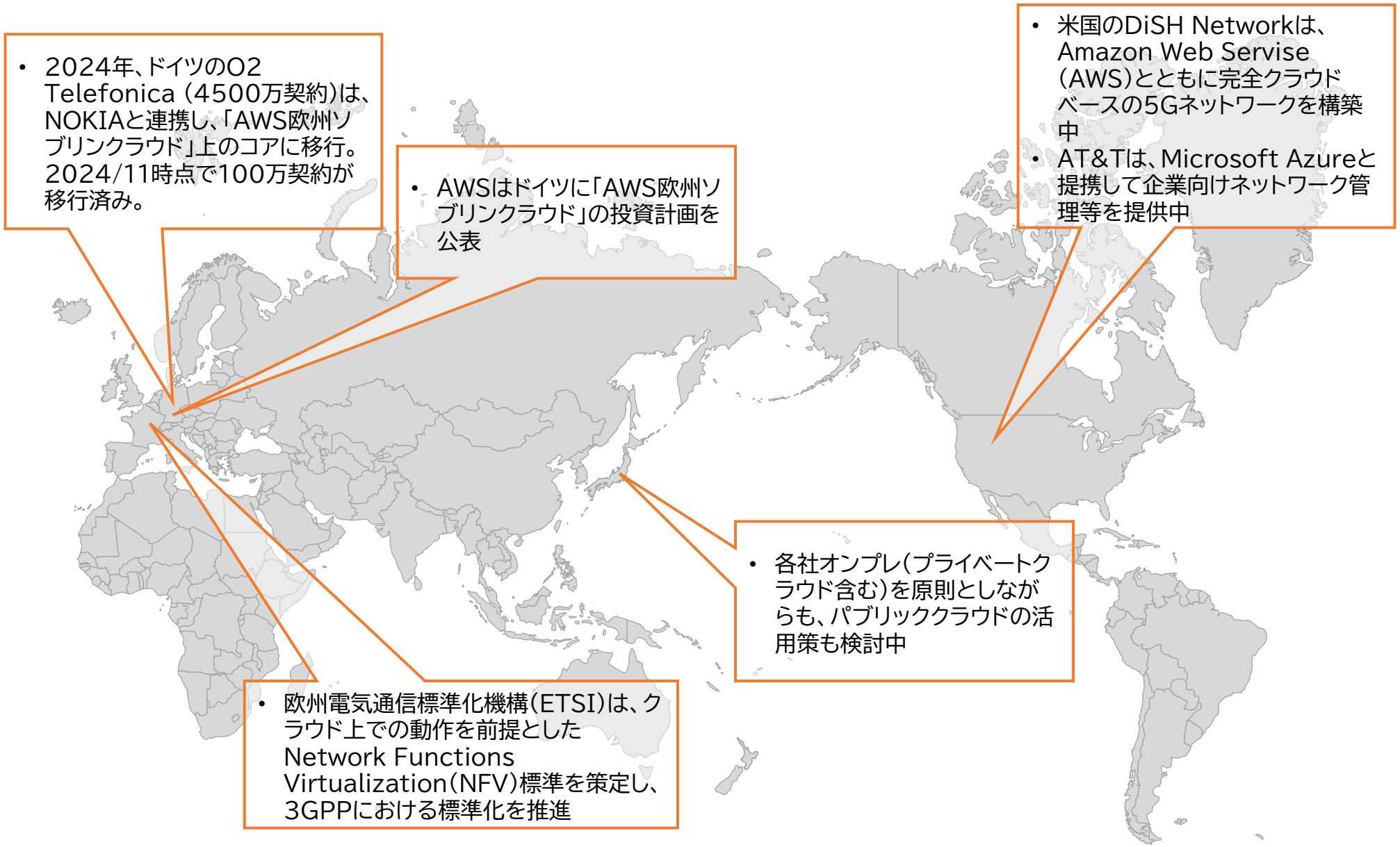


(出典)Synergy「Cloud Market Gets its Mojo Back; AI Helps Push Q4 Increase in Cloud Spending to New Highs」

(情報通信白書　令和6年版より)

- 世界のパブリッククラウドサービスへの支出額は2023年に5,636億ドルまで増加すると見込まれている(左上)。要因としては、ビジネスを展開する上でクラウドが不可欠なものになっていることに加え、生成AIを中心とした新技術の普及が挙げられる。生成AIについては、多様な業種への適用が考えられるものの、規模や特性に応じてカスタマイズ(アルゴリズム、コスト、主権、プライバシー、持続可能性等)が必要となるため、効果的に導入するためにはクラウドサービスの活用が見込まれる。

国内外の事例

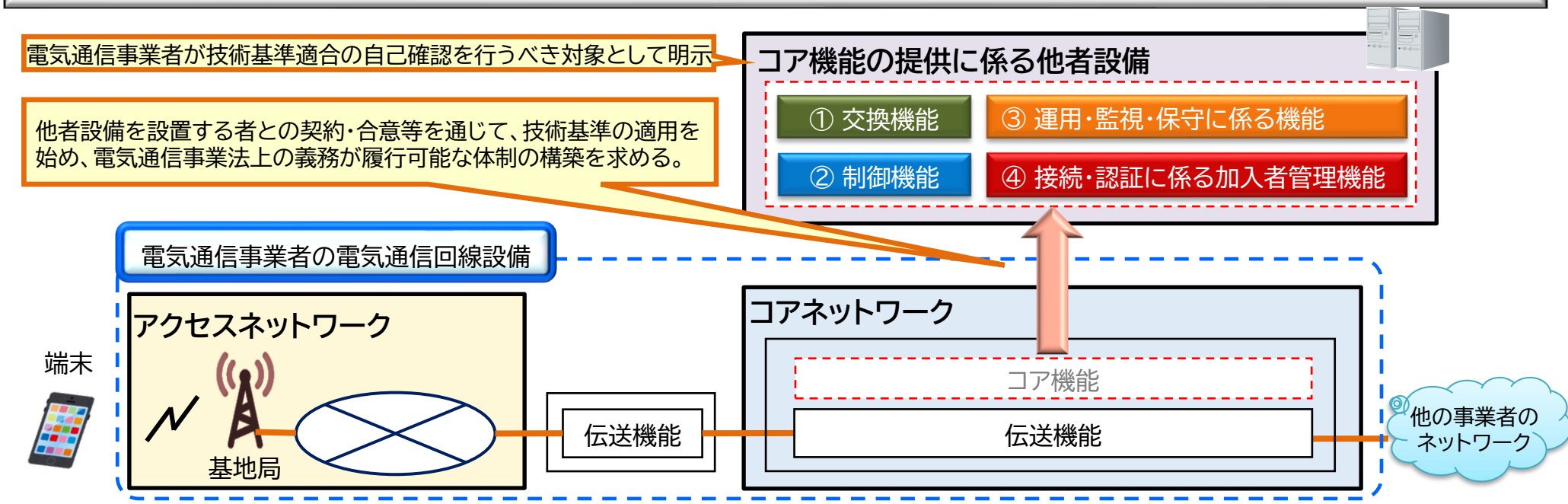

• 2024年、ドイツのO2 Telefonica（4500万契約）は、NOKIAと連携し、「AWS欧州ソブリンクラウド」上のコアに移行。2024/11時点で100万契約が移行済み。
• AWSはドイツに「AWS欧州ソブリンクラウド」の投資計画を公表
• 米国のDiSH Networkは、Amazon Web Servise（AWS）とともに完全クラウドベースの5Gネットワークを構築中
• AT&Tは、Microsoft Azureと提携して企業向けネットワーク管理等を提供中
• 各社オンプレ（プライベートクラウド含む）を原則としながらも、パブリッククラウドの活用策も検討中
• 欧州電気通信標準化機構（ETSI）は、クラウド上での動作を前提としたNetwork Functions Virtualization（NFV）標準を策定し、3GPPにおける標準化を推進

「電気通信事業法施行規則」等の改正（令和5年9月）の概要①

改正の主なポイント

- ①交換機能、②電気通信設備の制御機能（仮想化した機能を制御するための機能を含む。）、③電気通信設備の運用、監視又は保守に係る機能、④通信の接続又は認証に係る加入者管理機能を、重要な機能（以下「コア機能」という。）として特定。コア機能については、他者設備（クラウドサービスの提供に係る設備を含む。）を通じて提供される場合においても技術基準の適用対象とする。【施行規則第27条の2第3号】
- 事業用電気通信設備の自己確認の届出事項に、コア機能の提供に係る他者設備の管理に関する説明書を追加。【施行規則第27条の5第1号】
- 電気通信事業者が自ら定める管理規程の届出事項として、コア機能を提供する事業用電気通信設備の全部又は一部を構成する設備の運用を他人に委託している場合（クラウドサービス等を通じて他者からコア機能の提供を受ける場合を含む。）における業務管理体制に関する事項を追加。【施行規則第29条第1項】

※ あわせて、メタルインターネットプロトコル電話用設備と、インターネットプロトコルを用いた総合デジタル通信用設備について、事業用電気通信設備の自己確認の届出項目が明確になるように整理。（届出項目に変更を加えるものではない。）【施行規則第27条の5】



「電気通信事業法施行規則」等の改正（令和5年9月）の概要②

事業用電気通信設備の自己確認届出に関する記載マニュアル

- 総務省では、携帯電話用設備を例として、電気通信事業者が技術基準適合の自己確認届出書を作成する際の具体例を示した「電気通信事業法に基づく事業用電気通信設備（携帯電話用設備）の自己確認届出に関する記載マニュアル」を策定し、公表している。
- 今般の改正に合わせて、技術基準適合自己確認の対象となる設備（他者設備を含む。）の範囲を明確化するとともに、コア機能の提供に係る他者設備の管理に関する説明書の記載方法を追記。

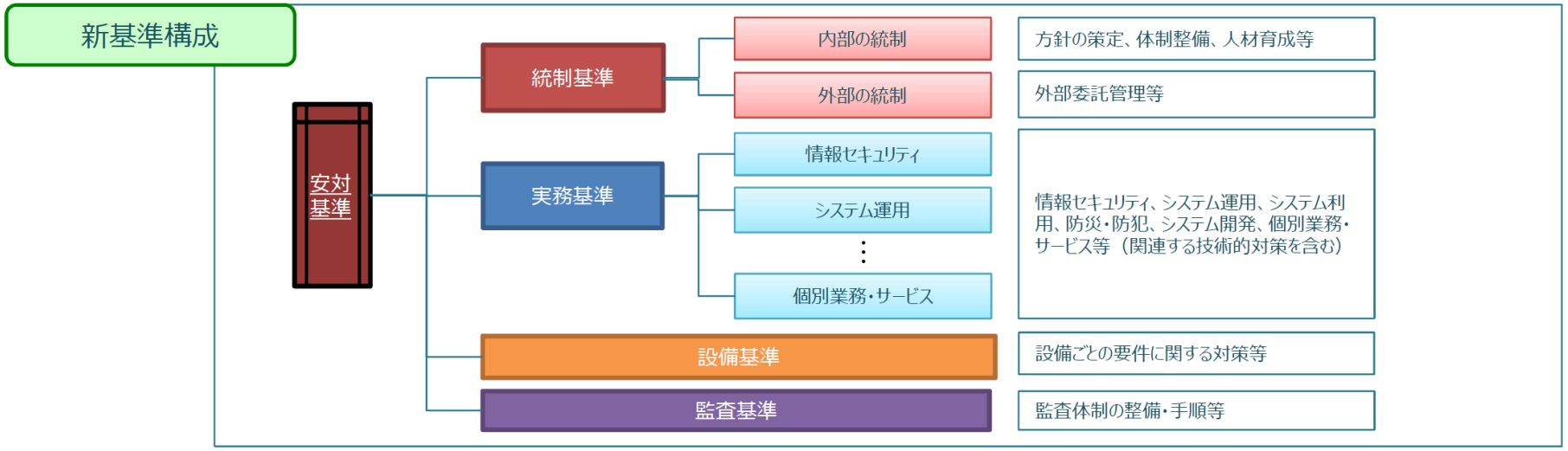
管理規程記載マニュアル

- 総務省では、電気通信事業者が自ら定める管理規程の各記載事項について具体例を示した「管理規程記載マニュアル」を策定し、公表している。
- 今般の改正に合わせて、コア機能を提供する事業用電気通信設備の全部又は一部を構成する設備の運用を委託している場合や、他者が提供するクラウドサービス等を通じてコア機能の提供を受ける場合に求められる業務管理体制の記載方法を追記。

金融分野におけるクラウド活用状況

－ 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」－

- 金融機関等の情報システムを取り巻く状況の変化を捉え、公益財団法人 金融情報システムセンター（FISC）では、外部委託に関する有識者検討会等を開催し、安全対策の方向性や諸課題をテーマに検討。その成果は、**「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」**としてとりまとめられ、令和6年3月に第12版が公表されている。
- また、同センターでは、クラウドサービスが高度化・多様化し、セキュリティリスクも高度化する中で、クラウドサービス固有の特性を踏まえた 、安全対策基準の適用の仕方に関する解説書として、令和3年5月に**「金融機関等におけるクラウド導入・ 運用に関する解説書（試行版）」**をとりまとめ、頒布している（当該解説書の内容は上記安全対策基準・解説書に既に取込み済）。



【金融機関等コンピュータシステムの安全対策基準の構成】

出典：「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12版）」（令和6年3月、同センター）
「金融機関等におけるクラウド導入・ 運用に関する解説書（試行版）」（令和3年5月、同センター）
https://www.fisc.or.jp/publication/guideline_pdf.php

金融分野におけるクラウド活用状況

－FISC「金融機関等におけるクラウド導入・運用に関する解説書（試行版）」（令和3年5月）より　－

- 本解説書において、クラウドシステムに対する安全対策を策定する上でポイントとされている主な内容は、以下の通り。

【クラウドサービスに対する安全対策を策定する上での留意点】

- クラウドサービスの責任分界点が提供形態により一義的に定まるものではないことを挙げ、金融機関とクラウド事業者との間の本分界点をしっかり確認した上で、金融機関が実施する安全対策を決定する必要があるとしている。
- クラウド事業者が実施する安全対策は金融機関が管理することが基本だが統制上の管理方法が制約される場合もあり、本統制については「クラウドサービスを外部委託の一形態としての観点」と「外部委託の観点に当てはまらないクラウドサービス固有の観点」と整理の上で、安全対策基準を示している（次項参照）。

【安全対策を策定する上で想定しているリスク】

- 経産省作成「クラウドセキュリティガイドライン活用ガイドブック」において整理された、クラウドシステムに関する一般的な脅威・リスク（25項目）に、金融分野特有のリスク（α～γの3項目）を加え（以下）、各項目に対して対策例をとりまとめている。

想定する脅威・リスクの分類と一覧			
インフラに関するリスクと対策	**ネットワーク**に関するリスクと対策	利用者との通信、サーバー間の通信	① 通信の傍受
		リージョン間の通信における脅威	② 中間者攻撃、③なりすまし
		コンピュータ環境におけるネットワーク上の脅威	④ ネットワーク管理の不備によるシステムダウン、 ⑤ VPNにおけるトラブルによるシステムダウン
	データセンターセキュリティに関するリスクと対策	物理的な攻撃	⑥ データセンターへの不正な入退館
			⑦ 機器への直接的な攻撃
		操作ミスなどの人的セキュリティ	⑧ 意図しない操作ミス、⑨ 内部関係者による意図的な攻撃
		電源に関する脅威と脆弱性	⑩ 電源の喪失によるサービス停止
仮想化基盤に関するリスクと対策	⑪ 事故に備えた対応の不備に対する対策		
サービス基盤に関するリスクと対策	⑫ 単一障害点となるサービスに関する脅威に対する対策、⑬ 共有サービスに関する脅威に対する対策		
統合管理環境に関するリスクと対策	⑭ 総合管理環境の脅威に関する対策、監視環境に関する脅威に対する対策		
データ管理に関するリスクと対策	**データ管理方針**に関するリスクと対策	⑮ データ管理におけるガバナンスの喪失に対する対策、 ⑯ 不正なデータの取得によるウィルス感染に対する対策	
	データ分類に関するリスクと対策	⑰ 適切なアクセス権の設定不能に対する対策	
	データのライフサイクル管理に関するリスクと対策	⑱ データ管理におけるライフサイクル管理の欠如に対する対策、 ⑲ データ漏洩・流出に対する対策	
	⑳ バックアップ		
ID管理に関するリスクと対策	㉑ クラウドにおけるID管理に関するリスクと対策、㉓ IDフェデレーションに関するリスクと対策		
人員に関するリスクと対策	㉔ クラウド利用者のリテラシーに関するリスクと対策、㉕ クラウド構築・運用・管理に関するリテラシーに関するリスクと対策		
α）ある事業者の提供しているクラウドサービスが、別の事業者のクラウドサービス提供を前提としている場合に、**金融機関等のガバナンス**が不十分になるリスク			
β）開発環境やテスト環境での作業により、本番環境での誤動作やパフォーマンスの低下など**本番業務に支障が発生**するリスク			
γ）**ガバナンスの喪失**により発生するリスク			

金融分野におけるクラウド活用状況

－FISC「金融機関等におけるクラウド導入・運用に関する解説書（試行版）」（令和3年5月）より　－

【「クラウドサービスの統制」に関する安全対策基準の内容】

- 「外部委託の一形態の観点」では、以下の【統20】～【統23】が該当し、クラウドサービスの**利用目的・範囲及び選定手続きの明確化**、クラウド事業者との**安全対策を盛り込んだ契約の締結**等を定めている。
- 「クラウド固有の観点」では、以下の【統24】が該当し、**クラウド拠点の把握**、契約書等への**監査権**の明記、**保証型監査報告書**の活用等を求めている。

基準中項目	基準番号	基準小項目	内　容
外部委託管理	統20	外部委託を行う場合は、事前に目的、範囲等を明確にするとともに、外部委託先選定の手続きを明確にすること。	適切な外部委託先を選定するため、外部委託を行う場合は、**事前に目的、範囲等を明確**にするとともに、**選定手続きを明確**にし、**外部委託先を客観的に評価**すること。また、外部委託先の決定にあたっては、責任者の承認を得ること。
	統21	外部委託先と安全対策に関する項目を盛り込んだ契約を締結すること。	安全性確保のため、**機密保護**、**安定的なシステム運用**等に関する項目を盛り込んだ契約を締結すること。
	統22	外部委託先の要員にルールを遵守させ、その遵守状況を確認すること。	セキュリティ管理を適切に行うため、外部委託先の要員に対し、委託業務の内容や作業の範囲に応じて、セキュリティポリシーをはじめとした**各種ルールの遵守を義務づけ、その遵守状況を確認**すること。
	統23	外部委託における管理体制を整備し、委託業務の遂行状況を確認すること。	外部委託先のセキュリティ管理状況及び、委託した業務が適切に遂行されているかを確認するため、委託業務の内容または作業の範囲に応じて、**外部委託管理体制を整備**するとともに、**委託契約に基づき委託業務の遂行状況を確認**すること。
クラウドサービスの利用	統24	クラウドサービスを利用する場合は、クラウドサービス固有のリスクを考慮した安全対策を講ずること。	クラウド事業者に対する統制を十分かつ実効的に機能させるため、クラウドサービスを利用する場合は、クラウドサービス固有のリスクを考慮した安全対策を講ずること。 例：統制対象のクラウド拠点やデータ保管場所の**所在の確認**、**サービス水準合意**の締結、**監査権**の明記、クラウド事業者が委託した**保証型監査報告書の利用**、**定期監査の実施**、対象のクラウドシステムに詳しい**専門知識を有する者の配置**、**責任分界点の明確化**　等

IPA「重要情報を扱うシステムの要求策定ガイド Ver. 1.0」（令和5年7月より）

- 本ガイドは、「重要情報を扱うシステム」の管理者が問題・リスクを分析し、その対策を自ら策定できることを目的としたもの。パブリッククラウドのみならず、プライベートクラウドやオンプレミスなどの形態も想定。
- 当該システムには、環境変化に追随するための「利便性」と、データ漏洩や改ざんの可能性、システム構成要素（ソフトウェア及びハードウェア等）のサプライチェーンを含めたシステムの安全性の確保、非平常時を含めたシステム運用の統制性や事態の収拾を図る結果責任を全うするための「自律性」の両立が求められる、とされている。
- なお、本ガイドは、金融機関向けFISC安全対策基準、政府向けISMAP管理基準等のシステムを構築する際の安全対策ガイドラインなどの内容を、上記の「利便性」と「自律性」の視点で補完するものとの位置づけ。

変化し続ける環境の中で、重要情報を扱うシステムのサービス安定供給

- **ビジネス**：変化し続けるビジネス環境への対応力の確保
- **技術**：進化し続けるシステム技術環境への対応力の確保

→ **利便性の確保**

- **ガバナンス**：国際環境やビジネス環境、技術環境の変化の中で、扱うデータや管理するシステムの安定化に向けた統制力の確保
  - **データ** の機密性・完全性・可用性確保のための項目
  - **運用** の完全性・可用性確保のための項目
  - **ソフトウェア** の完全性・可用性確保のための項目
  - **ハードウェア** の完全性・可用性確保のための項目
  - **データセンター・通信** の完全性・可用性確保のための項目

→ **自律性の確保**

→ 次ページ以降

IPA「重要情報を扱うシステムの要求策定ガイド Ver. 1.0」（令和5年7月より）

自律性（データの機密性・完全性・可用性）確保のための項目

重要情報を扱うシステムにおいて想定される問題やリスク	左記に対する対策	
• 運用者の不正によりデータが漏洩・改ざんされる • システムへの攻撃により大量にデータが漏洩する • 物理アクセスにより記憶媒体などが持ち出される • HWへの攻撃などで計算・データが漏洩する • 運用者の不正によりデータが破壊（消去）される • 運用者の操作誤りなどでデータが漏洩する	＜アクセス制限＞ • 運用者の権限制限 • システムへの強固なアクセス制限 ＜暗号化＞ • データの暗号化の確保 • 計算途上のデータ暗号化の確保 • システム基盤内通信路でのデータ暗号化の確保 • 外部通信路でのデータ暗号化の確保 ＜鍵管理＞ • 暗号鍵の安全・分離保存 • 暗号鍵のHW分離 • 暗号鍵管理の組織分離	＜冗長性＞ • データの冗長性の確保 ＜システムに備える機能＞ • アーカイブストレージの確保 • 誤設定を抑止する機能 • データ・システム混交を防止する機構設計 ＜情報の削除＞ • 情報の確実な削除 • 情報の論理的な削除 • 重要情報の物理的な削除 ＜情報の管理＞ • （インシデント発生時の）情報保存箇所の物理位置追跡・証跡管理

自律性（運用の完全性・可用性）確保のための項目

重要情報を扱うシステムにおいて想定される問題やリスク	左記に対する対策	
• 日本法と抵触する法体系による影響力でシステムが停止する・改ざんされる、データが回収不能になる・持ち去られる • 運用者の不正によりシステムが停止・改ざんされる • 大規模災害などで長時間停止・復旧不能になる • 障害対応に時間を要する／緩和策の実施が困難 • 立地施設が接収・干渉される • 運用組織が命令・干渉される • 運用者が命令・干渉される • 運用者の内部犯行 • 組織が日本法と抵触する法体系を強制される • 組織の資本支配者が外部から指示される • 運用者が日本法と抵触する法体系を優先適用する • 運用者が外部から干渉される • 運用体制が国内体制で完結していない	＜暗号化＞ • データの暗号化の確保 ＜暗号鍵の管理＞ • 暗号鍵の安全・分離保存 ＜冗長性＞ • データの冗長性の確保 • 運用体制の冗長性確保 ＜アクセス管理＞ • 運用操作の記録・監査・保全 • 人に対するセキュリティチェック ＜オンサイトの安全・信頼性＞ • 実地での立ち入り監査による実効性確保	＜国内主権の確保＞ • 運用体制への国内法の強制 • 運用体制の国内確保 • 資本・支配関係の比較法的チェック • 国内体制での障害および再発防止の対応 • データ持ち出しの可能性の確保（コスト面含む） ＜情報提供＞ • 運用状況の情報提供 • 障害などに対する対応と事後報告 ＜障害対応＞ • 管理者主導での障害などに対する対応

自律性（データセンタ・通信の完全性・可用性）確保のための項目

重要情報を扱うシステムにおいて想定される問題やリスク	左記に対する対策
• HWに物理アクセスできなくなる • HWに物理アクセスされる • HWにNWアクセスできなくなる • HWに不正にNWアクセスされる • 立地施設がアクセス不能になる • 立地施設にアクセスが強制される • アクセスできる権限者の内部犯行 • 立地施設に不適切な人のアクセスを許してしまう • 施設が想定外の被害を受ける • 外部通信経路が干渉される • 電力供給が止まる	＜オンサイトの安全・信頼性＞ • 機器の国内設置 • 電力供給の継続性確保 • 実地での立ち入り監査による実効性確保 ＜アクセス管理＞ • 適切な設備アクセスポリシーの強制 • 運用操作の記録・監査・保全 ＜システムの安全・信頼性＞ • 通信経路の信頼性確保 • データセンター・通信の冗長性確保 ＜国内主権の確保＞ • 日本法と抵触する法体系の設置箇所への適用の排除 ＜サプライチェーン＞ • サプライチェーンのセキュリティチェック • サブライチェーンの部品表管理 • サプライチェーンの継続的リスク評価

IPA「重要情報を扱うシステムの要求策定ガイド Ver. 1.0」（令和5年7月より）

自律性（ソフトウェアの完全性・可用性）確保のための項目

重要情報を扱うシステムにおいて想定される問題やリスク	左記に対する対策
• SWに不正な処理が混入する • SWの問題が適時に解決できない • SWの使用が継続できなくなる • システムの運用が不適時に停止する • SWの問題解決に必要な情報が提供されない • 脆弱性の対応が十分に入手できない • SWのメンテナンスが終息する • 法的な不安定性により取引ができなくなる	＜安全・信頼性＞ • SWの信頼性アセスメント • SWの継続的リスク評価 • 開発体制のセキュリティチェック • 脆弱性などへの対応 ＜維持管理対応＞ • SWのメンテナンスポリシーの確立（バージョン管理を含む） • メンテナンス処理への調整機構 • 商用SW（商用OSSを含む）への技術情報アクセスの確保 • 商用SW（商用OSSを含む）のメンテナンス性確保 • 自社開発SW・OSSに対する自社でのメンテナンス体制確保 ＜サプライチェーン＞ • サプライヤーのセキュリティチェック ＜資産管理＞ • SWの部品表管理 ※OSS：Open Source Software

自律性（ハードウェアの完全性・可用性）確保のための項目

重要情報を扱うシステムにおいて想定される問題やリスク	左記に対する対策
• HWの影響でシステム動作が改ざんされる • HWの影響でデータが盗聴される • HWの影響でシステム運用が停止する • 内部通信経路が干渉される • 外部通信経路が干渉される • HWの調達が止まる • HWの保守が止まる	＜安全・信頼性＞ • HWの信頼性アセスメント • HWの継続的リスク評価 • 脆弱性などへの対応 ＜サプライチェーン＞ • サプライヤーのセキュリティチェック • 複数の調達経路・部品選択肢の確保 ＜資産管理＞ • HWの部品表管理 • 調達部品のストック確保