

**令和3年度
重要技術管理体制強化事業
(クラウドを活用した重要情報管理
体制強化に向けた調査事業)**

調査報告書

ガートナー・ジャパン株式会社

本報告書目次

1. 調査概要（背景と目的、調査実施内容）
2. クラウドサービスに関する技術動向
3. 他国政府におけるクラウド利用状況
4. 重要情報を取り扱う企業等におけるクラウドサービスの利用実態・懸念点
5. 2021年度以降の施策展望・課題・対策

1. 調査概要（背景と目的、調査実施内容）

事業実施の基本方針、業務内容等：背景と目的

本事業では、クラウドサービスの利用実態や重要情報の取り扱い、今後利用拡大をする上での課題・懸念点についての調査・整理・分析を実施する

背景	状況理解	- 近年、技術革新を主導する民生技術と防衛技術の境界が曖昧となる中、懸念組織等への流出を防ぐ観点から情報管理の徹底が急務となっている - 特に、政府・産業・インフラ領域についてもクラウド化が進みつつあるが、高い安全性・信頼性をもって機密性の高いデータを扱えるクラウドサービスが充実しているとは言い難い状況にある
	対応の方向性	今後、政府・産業・インフラ領域において、セキュリティを担保しつつクラウドサービスの利用を進めていくために、利用者目線でどのような要件が求められているかを明らかにするとともに、今後必要とされるクラウドサービスの要素およびその実現に必要な技術課題を明らかにすることで、今後の研究開発や基準の策定等、社会実装支援に繋げていくことが必要である
目的	今後必要とされるクラウドサービスに関する情報収集	- 文献調査や有識者へのヒアリング調査等を通じて、クラウドサービス利用に関する最新の技術動向や企業の取り組み等を調査する - 重要情報を取り扱う企業に対し、アンケート調査・ヒアリング調査を通じて、クラウドサービス利用の現状や将来の利用拡大にあたっての懸念、クラウドサービスを積極的に活用している事例等を調査する - 各種調査結果をもとに、2021年度以降の施策展望・課題・対策等について明らかにする

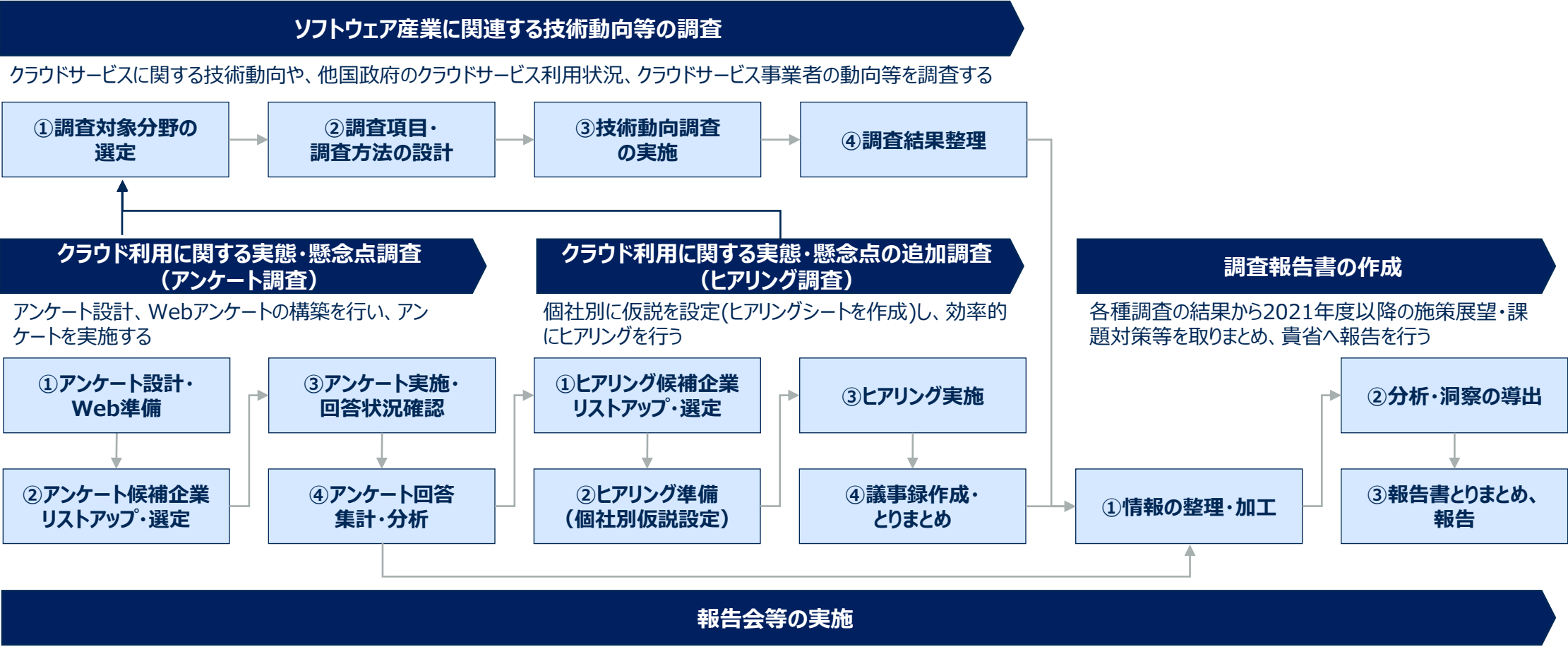
事業実施の基本方針、業務内容等：調査内容

クラウドサービスに関する最新の技術動向・取り組みと、クラウドサービスの利用実態および利用拡大にあたっての懸念と期待について、複数の調査を組み合わせること、実用的な調査結果を得る

セクション	調査目的	調査内容（検証したい主な論点）	調査アプローチ	
クラウドサービスに関する最新の技術動向、企業の取組等	クラウドサービスに関する最新の技術動向、企業の取組、他国の状況等の把握	- クラウドサービスの信頼性・安定性・利便性等を高める技術動向はどのようなものがあり、クラウドサービス事業者およびクラウドサービス利用者にとどのような影響を与えるか - 他国政府のクラウドサービス利用に関する現状や考え方は何か - クラウドサービス提供事業者側で行っている対応や戦略は何か	ソフトウェア産業に関連する技術動向等の調査 文献調査およびヒアリング調査	
クラウドサービスの利用実態	クラウドサービス利用に関する方針、利用状況・利用範囲、不満等の実態の把握	- クラウドサービス利用に関する戦略・方針はあるか - どのような業務領域について、どのようなクラウドサービスを利用しているか - クラウドサービス利用によってどのようなメリットを享受しているか - クラウドサービスを選定する上での基準はどのようなものがあるか - クラウドサービス利用に伴い、採用しているテクノロジーや取っている対策はどのようなものか - クラウドサービスを利用しない理由はどのようなものか - 現状のクラウドサービスに対して満足している点、不満な点は何か	クラウド利用に関する実態・懸念点調査	クラウド利用に関する実態・懸念点の追加調査
クラウドサービスの利用拡大にあたっての懸念と期待	- 将来のクラウドサービス利用の拡大にあたっての課題や懸念点の把握 - クラウドサービス事業者やテクノロジーへの期待の把握	- クラウドサービスの利用拡大に向け、どのような懸念点・課題があるか - 信頼性・安定性（災害対策・可用性、応答時間・超低遅延、セキュリティ、等） - 利便性・機能性（オープン性、運用のしやすさ、柔軟性、機能の多さ、等） - その他（ベンダーロックイン、国内法の適用、企業の持続可能性、環境負荷、等） - それぞれの懸念点・課題がどの程度解消されれば、利用拡大を検討するか - 懸念点・課題を解消する上で、クラウドサービス事業者やテクノロジーに期待することは何か		
			アンケート調査	ヒアリング調査

事業実施の基本方針、業務内容等：業務全体像

ソフトウェア産業に関連する技術動向等の調査、クラウド利用に関する実態・懸念点調査（アンケート調査）、クラウド利用に関する実態・懸念点の追加調査（ヒアリング調査）を行い、各種調査結果から2021年度以降の施策展望・課題対策等を調査報告書としてとりまとめる



2. クラウドサービスに関する技術動向

クラウドサービスに関する技術動向：調査項目

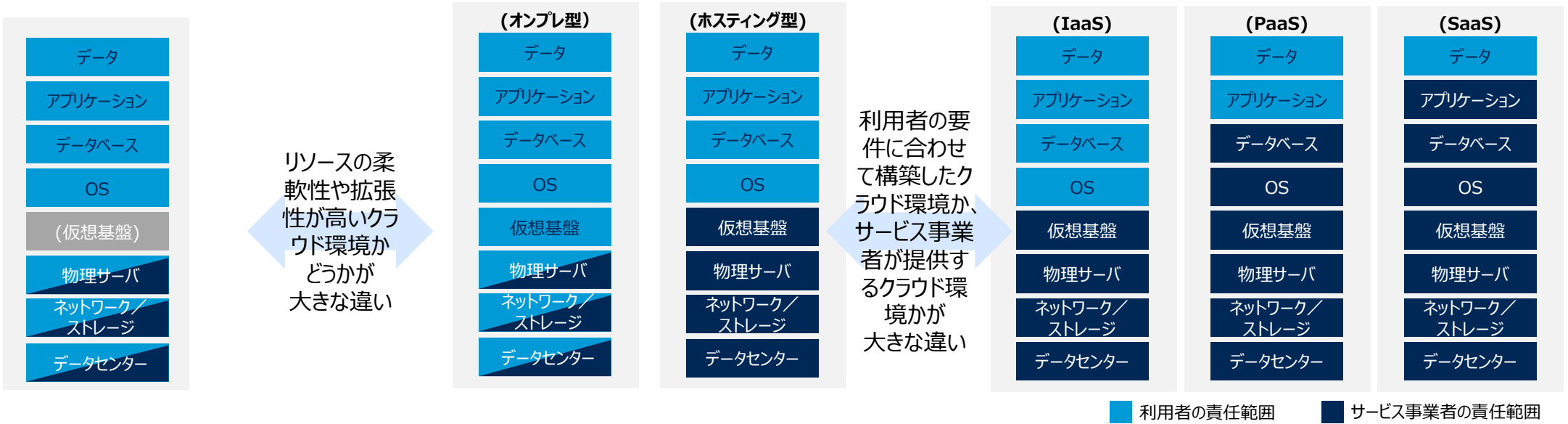
本調査では、クラウドサービスの比較及びクラウドサービス・技術のトレンドについて調査・整理を行う

項目	調査内容	調査方法
クラウドサービスに関する 技術動向	a) クラウドサービスの比較 クラウドの実装モデルごと（オンプレミス、プライベートクラウド、パブリッククラウド）の差異について、整理を実施する	・公表情報に基づく情報収集 ・文献調査
	b) クラウドサービスの最新トレンド クラウドサービス利用の期待や懸念解消を実現するクラウドサービスおよび技術のトレンド（マルチクラウド、ハイブリッドクラウド、分散クラウド、等）について、調査・整理を実施する	

調査a) クラウドサービスの比較 (1/3)

本調査において、利用者の要件に合わせて構築した情報システムがクラウド環境かどうか、クラウド環境が利用者の要件に合わせて構築したものかサービス事業者が提供するものか、の観点でオンプレミス、プライベートクラウド、パブリッククラウドを定義する

オンプレミス	プライベートクラウド	パブリッククラウド
- 利用者の要件に合わせてサーバ機器やソフトウェアを調達し情報システムを構築する形態 - 利用者のデータセンターに構築する形態、サービス事業者が提供するデータセンターに構築する形態（ハウジング）、サービス事業者が提供するデータセンターとハードウェアを利用して構築する形態（ホスティング）がある	- 利用者の要件に合わせてサーバ機器やソフトウェアを調達あるいはサービス事業者と契約し構築したクラウドサービスの形態 - 利用者がクラウド環境を構築するオンプレ型と、サービス事業者が所有するクラウド環境を利用者の要件に合わせて長期契約で利用するホスティング型がある	- サービス事業者がサービスメニューに基づき提供するクラウドサービスの形態 - サービス事業者が提供する範囲により主にIaaS、PaaS、SaaSの3つに分類される



調査a) クラウドサービスの比較 (2/3)

オンプレミスやプライベートクラウドは、利用者の業務要件に合わせたシステム・インフラ環境を構築することができるが、拡張性が低く、初期コストや運用コストが高価。パブリッククラウドは、拡張性が高く、初期コストや運用コストが安価であるが、サービス事業者への依存度が高く、カスタマイズ性が低く、障害発生時に即時対応や個別対応が難しい

	オンプレミス	プライベートクラウド(オンプレ型)	プライベートクラウド(ホスティング型)	パブリッククラウド
サーバの共有範囲	■ 利用者で専有	■ 利用者で専有	■ 利用者で専有 ■ 共有範囲において、他の利用者的高負荷な利用により、遅延等の影響がでる	■ 多数の利用者と共有 ■ 共有範囲において、他の利用者的高負荷な利用により、遅延等の大きな影響がでる
可用性	■ 利用者の可用性要件を実現できる ■ 高可用性を実現するには高コストとなる ■ 機器の障害時のフェイルオーバーや切り戻しの仕組みを利用者が導入し運用する	■ 利用者の可用性要件を実現できる ■ 高可用性を実現するには高コストとなる ■ 機器の障害時のフェイルオーバーや切り戻しの仕組みを利用者が導入し運用する	■ 機器の障害時はサービス事業者が用意するフェイルオーバーや切り戻しの機能を利用できる ■ サービス事業者の責任範囲について、事業者のSLAに従うため、可用性要件をクラウドサービスにあわせる必要がある	■ 機器の障害時はサービス事業者が用意するフェイルオーバーや切り戻しの機能を利用できる ■ 複数データセンターにサービスが分散され大規模災害発生時も事業継続が可能 ■ サービス事業者の責任範囲について、事業者のSLAに従うため、可用性要件をクラウドサービスにあわせる必要がある
機密性・完全性	■ 利用者のセキュリティポリシーに対応した高度なセキュリティ要件を実現できる ■ クローズドな環境に構築するため外部からの不正アクセスのリスクが少ない ■ データの暗号化やバックアップ等のセキュリティ対策を利用者が導入し運用するため負担が大きい	■ 利用者のセキュリティポリシーに対応した高度なセキュリティ要件を実現できる ■ クローズドな環境に専有環境で構築するため、外部からの不正アクセスのリスクが少ない ■ データの暗号化やバックアップ等のセキュリティ対策を利用者が導入し運用するため負担が大きい	■ サービス事業者の責任範囲は事業者の高度なセキュリティ対策が実施される ■ サービス事業者の用意するセキュリティ機能を利用できる ■ インターネット経由で接続できる場合、常にサイバー攻撃の脅威に晒される	■ サービス事業者の責任範囲は事業者の高度なセキュリティ対策が実施される ■ サービス事業者の用意するセキュリティ機能を利用できる ■ インターネット経由で接続できる場合、常にサイバー攻撃の脅威に晒される ■ データ保管場所の管理情報が不透明
初期コスト・運用コスト	■ システム構築後の固定費用での運用が可能で予算化しやすい ■ 機器等の準備が必要なため初期投資が大きい ■ 利用者側で管理・運用を行うため運用コストが高い	■ システム構築後の固定費用での運用が可能で予算化しやすい ■ 機器等の準備が必要なため初期投資が大きい ■ 利用者側で管理・運用を行うため運用コストが高い	■ 機器等の準備が不要なため初期投資を抑制できる ■ 初期費用やメンテナンス費用が別途発生する可能性がある ■ 長期間の契約となる場合が多い	■ 多くの場合は初期投資が不要 ■ 従量課金で適正なコストでサービス利用が可能だが、月額費用が変動するため予算が立てにくい

青字：メリット 赤字：デメリット

調査a) クラウドサービスの比較 (3/3)

オンプレミスやプライベートクラウドは、利用者の業務要件に合わせたシステム・インフラ環境を構築することができるが、拡張性が低く、初期コストや運用コストが高価。パブリッククラウドは、拡張性が高く、初期コストや運用コストが安価であるが、サービス事業者への依存度が高く、カスタマイズ性が低く、障害発生時に即時対応や個別対応が難しい

	オンプレミス	プライベートクラウド（オンプレ型）	プライベートクラウド(ホスティング型)	パブリッククラウド
拡張性・柔軟性・カスタマイズ性	- カスタマイズ性が高く、自社の業務内容やニーズあわせて最適なサーバを構築できる - リソース拡張にはサーバ追加が必要となり容易ではない	- カスタマイズ性が高く、自社の業務内容やニーズあわせて最適なサーバを構築できる - リソース拡張は容易だが、サーバ追加が必要な場合がある	- インスタンスやボリュームを必要なときに必要な分だけ使える - サービス事業者の責任範囲はサービス仕様に依存する - リソース拡張には契約変更が必要となる、リソース縮退はできない可能性がある	- 急激なサービス需要変化や業務見直しに伴うリソースの追加や変更が容易 - カスタマイズや自社システムとの連携には一定の制限がある - 提供サービスの増加に伴い適切なサービス選択が難しくなる - サービス事業者の個別機能の利用が進むとベンダーロックインのリスクがある
先進技術の活用	個別に先端技術を導入する必要がある	個別に先端技術を導入する必要がある	個別に先端技術を導入する必要がある	- 技術革新による新しい機能が随時追加され先端技術の活用が容易 - サービス事業者の独自性が高く、他社サービスとの互換性が低い
保守 (障害対応、計画停止等)	- 障害発生時は利用者で復旧対応を行う - 事後の原因究明・再発防止策の対応が可能 - システムメンテナンス等による計画停止時期は利用者が計画することが可能	- 障害発生時は利用者で復旧対応を行う - 事後の原因究明・再発防止策の対応が可能 - システムメンテナンス等による計画停止時期は利用者が計画することが可能	- 障害発生時は責任分界点に応じて利用者とサービス提供事業者が復旧作業を行う - サービス事業者の復旧対応について個別対応が困難な場合がある - システムメンテナンス等による計画停止時期は利用者が計画することが可能	- 障害発生時は責任分界点に応じて利用者とサービス提供事業者が復旧作業を行う - サービス事業者の復旧対応について利用者側で状況把握や個別対応は困難 - システムメンテナンス等の計画停止の実施時期等、個別の事前調整が難しい

青字：メリット 赤字：デメリット

調査b) クラウドサービスの最新トレンド -最新クラウドサービスの概説（1/2）

パブリッククラウドにおけるデータ保管場所やベンダーロックイン等の課題を解消するクラウドサービスや技術として、ハイブリッドクラウド、マルチクラウド、分散クラウド、インダストリークラウド、ソブリンクラウド、およびコンフィデンシャルコンピューティングが注目され、サービス事業者から関連サービスが提供され始めている

概説

1 Hybrid Cloud Computing (ハイブリッドクラウド)	パブリッククラウドとプライベートクラウドあるいはオンプレミスを組み合わせたクラウドの利用形態である
2 Multicloud (マルチクラウド)	複数のパブリッククラウドプロバイダーが提供するクラウドサービスを意図的に使用するクラウドの利用形態である
3 Distributed Cloud (分散クラウド)	パブリッククラウドをさまざまな物理拠点に分散させ、クラウド事業者がその運用、ガバナンス、アップデートに関する責任を負うクラウドの利用形態である
4 Industry Cloud (インダストリークラウド)	基盤となるクラウドサービスを活用し、特定の業界に特化した機能を提供するクラウドの利用形態である
5 Sovereign Cloud (ソブリンクラウド)	単一の地域内で提供される、データの居住性やその他の法的要件を満たすクラウドの利用形態である
6 Confidential Computing (コンフィデンシャル コンピューティング)	パブリッククラウドで処理中のデータをクラウド事業者であっても見ることはできない高いデータ保護に実現できる、エンクレーブとも呼ばれるハードウェアベースの信頼できる実行環境でコードを実行するセキュリティの仕組みである

調査b) クラウドサービスの最新トレンド -最新クラウドサービスの概説（2/2）

パブリッククラウドにおけるデータ保管場所やベンダーロックイン等の課題と、それらを解消するハイブリッドクラウド、マルチクラウド、分散クラウド、インダストリークラウド、ソブリンクラウド、コンフィデンシャルコンピューティングとの関係性を明確化する

パブリッククラウドの課題		① Hybrid Cloud Computing (ハイブリッドクラウド)	② Multicloud (マルチクラウド)	③ Distributed Cloud (分散クラウド)	④ Industry Cloud (インダストリークラウド)	⑤ Sovereign Cloud (ソブリンクラウド)	⑥ Confidential Computing (コンフィデンシャルコンピューティング)
サーバの共有範囲	共有範囲において、他の利用者の高負荷な利用により、遅延等の大きな影響がでる	○		○			
可用性	サービス事業者のSLAに従う	○	○				
機密性・完全性	データ保管場所の管理情報が不透明	○		○		○	
	インターネット経由で接続できる場合、常にサイバー攻撃の脅威に晒される						○
拡張性・柔軟性・カスタマイズ性	カスタマイズや自社システムとの連携には一定の制限がある	○	○				
	提供サービスの増加に伴い適切なサービス選択が難しくなる				○		
	サービス事業者の個別機能の利用が進むとベンダーロックインのリスクがある		○				
先進技術の活用	サービス事業者の独自性が高く、他社サービスとの互換性が低い		○				

調査b) クラウドサービスの最新トレンド -ハイブリッドクラウド／マルチクラウド

ハイブリッドクラウドは、利用者の要件に合わせプライベートクラウドとパブリッククラウドを柔軟に組み合わせて利用することで、プライベート／パブリック両方のメリットを提供する一方、システム構成や運用が複雑となるデメリットを有する。

マルチクラウドは、複数のクラウドサービスを組み合わせることで、ベンダーロックインのリスクを低減したり、特定要件に合わせて最適なサービスを選択できるメリットがある一方、システム構成や運用が複雑になったり、複数の契約が重なることで高コストになる可能性がある

① Hybrid Cloud Computing (ハイブリッドクラウド)

概要

- ハイブリッドクラウドとは、パブリッククラウドとプライベートクラウドあるいはオンプレミスを組み合わせたクラウドの利用形態である
- ハイブリッドクラウドは、プライベートクラウドの制御、コンプライアンス、セキュリティ、信頼性と併せて、パブリッククラウドのコスト最適化、俊敏性、柔軟性、スケーラビリティ、弾力性という、プライベート／パブリック両方の領域におけるメリットを活かしつつ、デメリットをカバーできる特徴がある

主なメリット／デメリット

- 重要システムはオンプレミスやプライベートで構築するなど、利用者の要件にあわせて柔軟にプライベート／パブリックを組合せることができる
- 複数のクラウドにシステムやデータを分けることで負荷分散やリスク分散効果がある
- システム構成や運用が複雑になる
- 全体のコスト管理が複雑になる

事例

- 日本航空株式会社、株式会社ゼンリンデータコム、等

② Multicloud (マルチクラウド)

概要

- マルチクラウドとは、複数のパブリッククラウドプロバイダーが提供するクラウドサービスを意図的に使用するクラウドの利用形態である
- マルチクラウドは、計画的マルチクラウド（ベンダーロックイン解消）、自然発生的マルチクラウド（複数のパブリッククラウドを自社で把握せずに利用）、発展的マルチクラウド（必要に応じて別のパブリッククラウドを利用）、先端的マルチクラウド（コンテナ技術による利用）の4つに分類できる
- マルチクラウドは、特定クラウド事業者によるロックインのリスクを低減する可能性が期待されており、特定のユースケースに最適な機能を提供する

主なメリット／デメリット

- 要件にあわせて最適なサービスを選択できカスタマイズ性が向上する
- ベンダーロックインのリスクを軽減できる
- システム構成や運用が複雑になる
- 複数の契約が重なり高コストになる可能性がある

事例

- ヤマトホールディングス株式会社、株式会社ZOZOテクノロジーズ、等

調査b) クラウドサービスの最新トレンド -分散クラウド／インダストリークラウド

分散クラウドは、パブリッククラウドをさまざまな物理拠点に分散させクラウドサービスが提供されるもので、データに関する規制の問題を解決でき、低遅延やネットワーク関連障害への耐性強化などのメリットがある一方、利用者内に導入しデータ管理する場合は、データのバックアップ・リカバリの運用は利用者側で検討が必要となる・インダストリークラウドは、基盤となるクラウドサービスを活用し、特定の業界に特有の機能、規制などに対応するサービスを包括的に提供することで、調達や実装のプロセスを簡素化できるが、サービス事業者がサービスアップグレードをしない、あるいは新サービスとの互換性を確保しない場合は古いサービスを使用することになる

③ Distributed Cloud (分散クラウド)

概要

- 分散クラウドとは、パブリッククラウドをさまざまな物理拠点に分散させ、クラウド事業者がその運用、ガバナンス、アップデートに関する責任を負うクラウドの利用形態である
- 分散クラウドには様々なアプローチがある（ソフトウェアによるアプローチ、アプライアンスによるアプローチ等）
- 分散クラウドによって、企業は、どこでも必要な場所で、一貫性のあるクラウドコンピューティングを利用できる

主なメリット／デメリット

- データのロケーション、セキュリティとプライバシー、規制上の問題を解決できる可能性がある。
- 低遅延のクラウドコンピューティング実現、パフォーマンスが大幅に向上するだけでなく、ネットワーク関連障害が発生するリスクが軽減される
- 利用者内に導入しデータ管理する場合、データのバックアップ、リカバリの計画は利用者側で検討が必要になる

事例

- 国内では、ソフトバンク株式会社がIBMと共同検証を実施
- 海外では、Lumen Technologiesの事例がある

④ Industry Cloud (インダストリークラウド)

概要

- インダストリークラウドは、基盤となるクラウドサービスを活用し、特定の業界に特化した機能を提供するクラウドの利用形態である
- 対象となる業界に特有の機能、規制、技術の要件やユースケースに対応し、必要なサービスを包括的に提供する
- コミュニティクラウドと同義として使われる場合もある
- 従来は別々に提供していたクラウドサービスを事前に統合されたソリューションにまとめることで、利用者は、調達、実装、統合のプロセスを簡素化できる

主なメリット／デメリット

- 利用者は1からアーキテクチャを設計する必要がなくなる
- サービス事業者がサービスをアップグレードをしない、あるいは新サービスとの互換性を確保しない場合、古いサービスを長期間使用することになる
- サービス事業者や導入・運用をサポートするSierは、SaaS／PaaS／IaaSのクラウドサービスのスキルだけでなく、各業界の知見やノウハウが必要になる

事例

- 海外では、公共／製造業／小売／医療／農業の各業界で導入が進む
- 国内では、放送業界向けや自動車部品メーカーの事例がある

調査b) クラウドサービスの最新トレンド

-ソブリンクラウド／コンフィデンシャルコンピューティング

ソブリンクラウドは、単一地域内で提供され、データの居住性やその他の法的要件を満たすクラウドサービスであり、様々な国や地域でのデータ保護に関する規制要件に対応できるが、データ保護に関する国際動向の変化により、一時的な利用となる可能性がある。

コンフィデンシャルコンピューティングは、ハードウェアベースの信頼できる実行環境でコードを実行するセキュリティの仕組みであり、パブリッククラウド上でのデータ利用の安全性が向上するが、技術の複雑さにより実装方法が困難になる、さらには利用コストが増大する可能性がある

⑤ Sovereign Cloud (ソブリンクラウド)

概要

- ソブリンクラウドは、単一の地域内で提供される、データの居住性やその他の法的要件を満たすクラウドの利用形態である
- データが外部の司法権の支配を受けないことを保証し、各国の法律で強制されたアクセスからの保護を提供する
- ソブリンクラウドを採用することで、各国におけるデジタルおよびデータの主権を実現し、データ保護管理とアクセス制御、および情報収集するためのルールと法的要件の準拠性を確保する

主なメリット／デメリット

- 様々な国や地域でのデータ保護に関する規制要件に対応できる
- データ保護に関する国際動向の変化（例えば、米国とEUが国境を越えたデータ要求の処理方法に関する国際条約に合意した場合）により、ソブリンクラウドは一時的な利用となる可能性がある

事例

- ドイツやフランスなど欧州で導入が進み、ドイツでは公共／自動車／ヘルスケアの業界で導入

⑥ Confidential Computing (コンフィデンシャル コンピューティング)

概要

- コンフィデンシャルコンピューティングとは、エンクレープとも呼ばれるハードウェアベースの信頼できる実行環境でコードを実行するセキュリティの仕組みである。エンクレープはコードとデータをホストシステム（およびホストシステムの所有者）から分離して保護しコードの整合性と認証を提供する
- データ保管時の暗号化やデータ伝送時の暗号化に加え、処理中のデータの暗号化により、常にデータの暗号化を維持できるため、物理的にアクセス可能なサービス事業者からもデータの機密性が確保でき、クラウド環境のセキュリティとプライバシーを強化できる

主なメリット／デメリット

- プライバシー情報をシステム開発者やサービス運用者からも暗号化したまま、データ分析が可能となり、データ利活用とプライバシー保護の両立を実現する
- クラウド事業者を信頼せずにクラウド環境でデータ保管や処理が可能になるゼロトラストを実現する
- 異業種など複数の企業間で、機密情報の内容を明かすことなくクラウド上でデータ連携が可能となりDX推進に寄与する
- 技術の複雑さのため実装方法の十分な理解が困難な可能性がある
- 利用コストが増大する可能性がある

事例

- AWSとGoogleはサービス提供開始、Microsoftはパブリックプレビュー段階

3. 他国政府におけるクラウド利用状況

他国政府におけるクラウド利用状況：調査項目

本調査については、各国のクラウド利用方針と促進施策およびクラウドの利用状況について調査・整理を行う

項目	調査内容	調査方法
他国政府におけるクラウド利用状況	a) 他国政府におけるクラウドサービスの利用方針 他国政府におけるクラウドサービスの利用方針や戦略、ガイドライン等について、各国特有の事情や背景を踏まえた特徴や違いを調査する	・公表情報に基づく情報収集 ・文献調査 ・有識者ヒアリング
	b) 各国のクラウドサービス利用の促進施策 各国におけるクラウド利用を促進する施策・制度・仕組み等について、各国特有の事情や背景を踏まえた特徴や違いを調査する	
	c) 各国のクラウドサービス利用状況 各国における政府系システムのクラウドへの移行状況（どのようなシステムのクラウド利用が進んでいるか、どのようなシステムは進んでいないか）などの概況とその背景・理由などを調査する	

調査対象国選定の考え方

国連電子政府ランキング／早稲田大学世界デジタル政府ランキングの上位国が、クラウド利用も進んでいる国であると想定し、調査対象国を選定する。国連電子政府ランキングは「政府」のデジタル化の状態そのものを指しているわけではないことから、早稲田大学世界デジタル政府ランキングの評価指標の中で、クラウド利活用度を調査している「先端ICTの利活用度」の評価が高い、**米国**、**シンガポール**、および**英国**を調査対象国とする

国連電子政府ランキング2020年

順位	国・地域
1	デンマーク
2	韓国
3	エストニア
4	フィンランド
5	オーストラリア
6	スウェーデン
7	英国
8	ニュージーランド
9	米国
10	オランダ
11	シンガポール
12	アイスランド
13	ノルウェー
14	日本
15	オーストリア
：	：

出典：E-Government Survey 2020※1

早稲田大学世界デジタル政府ランキング2021年

順位	国・地域
1	デンマーク
2	シンガポール
3	英国
4	米国
5	カナダ
6	エストニア
7	ニュージーランド
8	韓国
9	日本
10	台湾
11	オーストラリア
12	スウェーデン
13	フィンランド
14	オランダ
15	スイス
：	：

出典：早稲田大学世界デジタル政府ランキング2021※2

主要分野評価指標とサブ指標リスト

審査大項目	審査小項目
ネットワーク・インフラの充実度・NIP （公的ネットワークの構築・整備）	1-1 インターネット加入者 1-2 ブロードバンド・ユーザー 1-3 デジタル携帯電話加入者
行財政改革への貢献度，行政管理の最適化・ MO（EA などの効果）	2-1 最適化進捗度 2-2 統合 EA モデル 2-3 行政管理予算システム
：	：
先端 ICT の利活用度・EMG	10-1 クラウド利活用 10-2 IoT 利活用 10-3 ビッグデータ利活用

先進ICTの利活用度（EMG）

順位	国・地域	EMG-Score
1	米国	7,500
2	シンガポール	7,000
2	英国	7,000
4	カナダ	6,500
：	：	：

※1 <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020>
※2 https://idg-waseda.jp/pdf/2021_Digital_Government_Ranking_Press_Release_Japanese.pdf

調査a) 他国政府におけるクラウドサービスの利用方針

米国は、2010年に発表した「クラウド・ファースト戦略」のフォローアップを実施し、2019年に「クラウド・ファースト戦略」を更新する「クラウド・スマート戦略」を導入。「クラウド・スマート戦略」ではクラウドサービス利用の評価の必要性に言及するとともに、クラウドサービス利用で焦点とすべきセキュリティ、調達、および労働力に関するガイダンスを提供している

米国におけるクラウドサービス利用方針の最新動向

・ 2019年に「クラウド・ファースト戦略」を更新する「クラウド・スマート戦略」を導入※1、より詳細なガイダンスを提供

- 米国連邦政府に対し、データセンターの統合にとどまらず商用クラウドサービス利用を推進
- アプリケーションをオンプレミスからクラウドにそのまま移行しても必ずしもクラウドのメリットを享受できるとは限らず、投資前にアプリケーションを置き換える等のコストやセキュリティリスクを評価する必要性を言及
- 政府機関は、クラウド利用を想定したセキュリティ設計がされていない、サービスレベル交渉や従量課金モデルを採用できない、IT人材はクラウドを最大限活用するためのスキルやトレーニングが不足している、等の課題を提起し、ガイダンスを提供

セキュリティ ガイダンス例

- データレベルの保護、継続的なモニタリング、信頼されたインターネット接続のポリシー準拠、暗号化、アイデンティティ・クレデンシャル・アクセス管理、ログファイルへのアクセス、サードパーティ、インシデント通知、継続的な診断と緩和の利用、FedRAMPの相互運用性とスピード

調達 ガイダンス例

- クラウドに情報を保存する可能性のあるサービス契約には注意が必要
- ベンダーロックインを避ける
- 事業継続と災害復旧に対応する
- カテゴリ管理(ベストインクラス/政府全体の買収契約の使用)
- サービスレベル契約(役割と責任、パフォーマンス指標、改善計画などを盛り込む)
- 価値の高い資産には、プライバシーとセキュリティの継続的な可視化が必要

労働力 ガイダンス例

- CIO、CHO、プライバシー担当上級職員が共同でスキル・ギャップを特定
- 新しいスキルと従来の職業分類を分析
- 業界予測を活用する
- NICEフレームワークの活用
- 技術系、非技術系のスキルアップ戦略の策定
- リスキルしたスタッフのための再配置オプションの開発
- 継続的な教育の計画 - 継続的なリスキル
- リスキルに対する責任者からの全面的な支援
- 採用戦略の更新 - 民間企業の手法の活用
- 変化に関するコミュニケーションプランの実行

出典：有識者ヒアリングをもとに作成

調査a) 他国政府におけるクラウドサービスの利用方針

英国は、2013年に「クラウド・ファースト戦略」を導入し、パブリッククラウドサービスの利用を優先させ、政府情報システムのクラウド利用を促進している。「クラウド・ファースト戦略」のフォローアップを実施し、2020年にクラウドサービス利用の問題に対処するクラウド利用ガイドを発表している

英国におけるクラウドサービス利用方針の最新動向

- **2011年に「政府ICT戦略」の1つとして「政府クラウド戦略」を発表※1**

- 「政府ICT戦略」の共通ICTインフラストラクチャの具体的策として「政府クラウド戦略」を発表
- 政府アプリケーションストア（オープンマーケットプレイス）を構築し、政府機関に対し政府が認証したクラウドサービスを提供
- 政府機関のクラウドサービスの調達効率化と中小企業による政府アプリケーション等市場への参入の容易化を実現

- **2013年に「クラウド・ファースト戦略」を導入※2**

クラウドサービスを優先して検討

- 新規または既存のサービスを調達する場合、政府機関は他の選択肢を検討する前に、まずクラウドサービスの可能性を検討し、十分に評価する必要がある
- 政府機関はクラウド以外の代替案を自由に選択できるが、より優れたコストパフォーマンスを提供することを証明する必要がある

パブリッククラウド・ファースト

- 「クラウド・ファースト戦略」では、コミュニティクラウド、ハイブリッドクラウド、またはプライベートクラウドではなく、パブリッククラウドの導入を検討する。

- **2020年に政府機関のクラウド活用ガイド（The One Government Cloud Strategy）を公表※3**

- 「クラウド・ファースト」戦略のフォローアップを実施し、ベンダーロックイン、クラウドサービス、技術、セキュリティ、運用、および人材等の課題に対するガイダンスや事例を提供

調査a) 他国政府におけるクラウドサービスの利用方針

シンガポールは、他国政府（英国、オーストラリア、ニュージーランド）が政府情報システムをクラウドに移行している状況をふまえ、2018年に発表された、「スマート・ネーション構想」の重要分野の1プロジェクトであるCODEXにおいて、政府情報システムをオンプレミスからパブリッククラウドへの移行を進めている

シンガポールにおけるクラウドサービス利用方針の最新動向

- **2014年に「スマート・ネーション構想」を発表※1**
- **2018年にクラウド移行を促進するCODEXプロジェクトを発表※2**
 - 「スマート・ネーション構想」では、最新のデジタル技術活用して国全体のスマートシティ化を実現し社会課題の解決とビジネスの創出を目指している
 - 重要分野として、開始当初は5分野を特定し、以降、3分野が追加され、戦略的国家プロジェクトとして推進している
 - 2018年に追加されたCODEX（Core Operations Development Environment and eXchange）プロジェクトにて、大半の政府システムをオンプレミスからパブリッククラウドに移行させる5か年計画を発表

CODEXは、より優れた、より高速で、より費用効果の高いデジタルサービスを開発するための、政府機関と民間部門で共有されるデジタルプラットフォーム※3

CODEXの構成：

- ① データの標準化や共通フォーマットにより政府機関間でのデータ共有を可能にする政府データアーキテクチャの策定
- ② 機密性の低い政府情報システムやデータのパブリッククラウドへの移行
- ③ ソフトウェアやインフラなどのデジタルコンポーネントを共有可能とするシンガポール政府技術スタック（SGTS）の構築

調査a) 他国政府におけるクラウドサービスの利用方針 – 情報分類

米国と英国は、政府が保持する情報を分類しており、UNCLASSIFIED／CONTROLLED UNCLASSIFIED INFORMATION（米国）、OFFICIAL／OFFICIAL-SENSITIVE（英国）に分類された情報はパブリッククラウドに保存できるとしている

米国における情報分類

UNCLASSIFIED 許可なしに公開できる情報
CONTROLLED UNCLASSIFIED INFORMATION - UNCLASSIFIEDの情報で、情報公開が管理されるべき情報（研究開発の技術情報等） - 多数のサブカテゴリで分類する（例、LAW ENFORCEMENT SENSITIVE）
CONFIDENTIAL 国家安全保障に損害を与えることが合理的に予想される情報
SECRET 国家の安全保障に重大な損害を与えることが合理的に予想される情報
TOP SECRET 国家安全保障に極めて重大な損害を与えることが合理的に予想される情報

出典：有識者ヒアリングをもとに作成

パブリッククラウドに保存できる情報

英国における情報分類

OFFICIAL 一般行政、公安、刑事司法、法執行などの政府の日常的な業務やサービスに関する情報で、情報の大部分（約90%）に適用される
OFFICIAL-SENSITIVE - OFFICIALの情報で特別な取り扱いを必要とする情報 - 厳密なアクセス制御を実施する
SECRET SENSITIVE - 国家安全保障やテロ対策、重大犯罪、個人の生命や自由への脅威など、軍事力や国際関係、または深刻な組織犯罪に関する情報に適用される - 安全な場所にのみ保存する必要がある。通常、SECRET SENSITIVEの情報をデータセンターに保存するには、英国内に配置し、適切なセキュリティ対策を講じる必要がある
TOP SECRET - 最も機密性の高い情報であり、広範囲にわたる人命損失を引き起こす、あるいは友好国の安全や経済を脅かす情報に適用される - 高度なセキュリティクリアランスを持つ担当者のみが安全にアクセスできる場所など、トップシークレットの保管場所として評価された安全な場所にのみ保管する

出典：有識者ヒアリングをもとに作成

パブリッククラウドに保存できる情報

調査b) 各国のクラウドサービス利用の促進施策

米国連邦政府は、「クラウド・ファースト戦略」の推進をサポートするため、各政府機関が導入するクラウドサービスの安全性を評価するプログラム（FedRAMP）を立ち上げ、認証プロセスの一貫性や効率性を確保している。認証を受けたクラウドサービスはあらゆる連邦政府機関で導入可能なサービスとしてみなされる

■ FedRAMP (Federal Risk and Authorization Management Program)

特徴	
発表／ 運用開始時期	2011年12月発表 2012年6月運用開始
内容	- 米国連邦政府のクラウドサービス調達のためのリスクおよび認証管理プログラム - クラウドサービス事業者が、このプログラムの認証を受けて登録されると、政府機関ごとに新たな調達評価の手続きを経ることなく、クラウドサービスを提供／調達することが可能な仕組み
認証申請	- 合同承認員会であるJoint Authorization Board（JAB）が許可する方法と、政府機関が認可する2つの方法がある - 評価基準はNIST-SP 800-53をベースに策定、実装する必要があるコントロールはFedRAMP Security Controls Baselineに規定
認証単位	サービス単位で認証 例. AWS GovCloud; Azure Government; Office 365 Multi; Cisco Webex

動向
2022年1月時点の認証サービス数は247※¹で、サービス事業者の数は279。2018年12月時点では認証サービス数は126であり、この3年間で認証サービス数は2倍に増加している 2012年に運用開始されて以降、認証取得にかかる期間が長く、高いコストが問題視されてきた。平均的な認証期間は18か月、コストは承認で250万ドル、監査で年間100万ドル※²。また、コストは提供費用に転嫁されていることが指摘されている - これらの課題を解消するため、2016年に「FedRAMP Accelerated※³」プログラム（3～6か月に短縮、承認コストは25万ドルから75万ドルを目指す）や低リスクSaaS サービスを対象とする「FedRAMP Tailored※⁴」プログラム（4～8週間に短縮、承認コストは3万ドルから4万ドルを目指す）を発表するなど、認証申請プロセスを効率化するために取り組みを行っている。また、審査の自動化にむけ、NISTと連携し、事業者のセキュリティ管理策を機械可読な形式で記述するOpen Security Controls Assessment Language（OSCAL）を2021年に開発※⁵、審査への適用に向けた取組みを継続検証している

※1 <https://marketplace.fedramp.gov/>

※2 <https://digital.gov/2016/09/16/how-much-does-it-cost-to-go-through-fedramp/>

※3 https://www.fedramp.gov/assets/resources/documents/FedRAMP_Accelerated_A_Case_Study_For_Change_Within_Government.pdf

※4 <https://www.fedscoop.com/fedramp-launches-tailored-baseline/>

※5 <https://www.fedramp.gov/FedRAMP-moves-to-automate-the-authorization-process/>

調査b) 各国のクラウドサービス利用の促進施策（1/2）

英国政府は、「クラウド・ファースト戦略」の推進をサポートするため、調達フレームワーク（G-Cloud framework）を導入し、政府機関によるクラウドサービスの調達を容易にしている。デジタルマーケットプレイスを提供し、政府機関はデジタルマーケットプレイスを介してサービス事業者からサービスを購入できる

■ G-Cloud framework（Government Cloud framework）

特徴	
発表／ 運用開始時期	2011年3月発表 2012年運用開始
内容	- 英国政府が運営する、政府機関向けクラウドサービスの調達フレームワーク - クラウドサービスのサプライヤー（AWSやMicrosoft など）との一連のフレームワーク契約と、オンラインストアであるデジタルマーケットプレイスでのサービスの一覧で構成される - 全てのクラウドサービスはG-Cloud Frameworkを介して購入する必要がある
認証申請	クラウドセキュリティ14原則について自己評価を行い、対象となるサービスがその原則に準拠していることを証明するドキュメントを準備した上で、証拠を提出する
認証単位	サービス単位で認証 （例. Amazon RDS; Google Kubernetes Engine; Google CDN; Microsoft Unified Support）

動向
- Framework Agreementにより基本的な契約事項がカバーされ、調達プロセスの簡素化により、迅速に契約や提供が可能なことから利用が進んでいる 2022年1月時点で、3つのサービスカテゴリ（クラウドホスティング、クラウドソフトウェア、クラウドサポート）があり、全体で約4万のサービスが登録されている※1 - 昨年度の売上は2.3billionポンドで、前年比で約30%増加している※2 - SME（中小企業）の売上が全体の約39%を占め、SMEも政府調達へ参入できる機会を創出している※2

調査b) 各国のクラウドサービス利用の促進施策（1/2）

シンガポール政府は、2018年に発表した政府情報システムのクラウド移行促進プロジェクト（CODEX）以前より、クラウドサービスのセキュリティ評価・認証制度「MTCS SS」を導入し、業界全体でのクラウド導入を促進している

■ MTCS SS（Multi-Tier Cloud Security Singapore Standard）

特徴	
発表／ 運用開始時期	2012年発表 2013年運用開始
内容	- シンガポール政府で運用されているセキュリティ管理規格 - 認証取得が政府のパブリッククラウドの一括入札参加の要件になる、認証されたサービスは金融業界等の関連規制で要求されるコントロールの検証が不要となる
認証申請	- 認定された認証機関による第三者認証、および自己開示文書（データ保持、可用性、BCP/DR等）の提出 - 認証は3年間有効、毎年審査が実施される - 評価基準はISO 27001/02 ISMSに基づく
認証単位	サービス単位 （例. Google LLC Google Cloud Platform; Microsoft Azure Compute; Microsoft Office Web Applications）

動向
2022年1月時点で、2つのサービスカテゴリ（IaaS／PaaS、SaaS）があり、全体で149のサービスが登録されている。2017年4月時点で認証サービス数は90であり、この5年間で認証サービス数は1.5倍に増加している※1 2015年に業界ヘフィードバックを求め、セキュリティ保証の明確化、監査手順の厳密化等の規格の一部の項目を更新している※2 - 最新版は2020年に公開され、用語の定義、監査手順の標準化、コンテナ等のクラウドサービスへの対応、等が追加された※3

※1 <https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Compliance-and-Certification>

※2 <https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Cloud-Computing-and-Services>

※3 <https://www.imda.gov.sg/news-and-events/Media-Room/archived/ida/Speeches/2015/speech-by-ida-assistant-chief-executive-mr-khoong-hock-yun-at-cloudasia-2015>

調査a,b) 各国のクラウドサービス利用方針・促進施策 -各国比較

米国、英国、およびシンガポールと同様に、日本国政府も「クラウド・バイ・デフォルト原則」のもと、政府情報システムへのクラウド利用を促進している。また、クラウドサービス選定制度（ISMAP）を2021年から開始し、2022年1月時点で34のサービスが認証を取得している

	米国	英国	シンガポール	日本
クラウド利用の 戦略・計画	「クラウド・スマート戦略」（2019年） 「クラウド・ファースト戦略」（2011年）のフローアップを実施し、「クラウド・ファースト戦略」を更新 - クラウドサービス利用を成功させるための3つの主要領域（セキュリティ、調達、労働力）のガイダンスを提供	「クラウドファースト戦略」（2013年） - クラウドサービスを優先して検討、クラウド以外の代替案についてはより優れたコストパフォーマンスを提供することを証明する必要がある - コミュニティクラウド、ハイブリッドクラウド、またはプライベートクラウドではなく、パブリッククラウドの導入を検討	「スマート・ネーション構想（CODEX）」（2018年） 5か年計画で機密性の低い政府情報システムやデータの大半をパブリッククラウドに移行	「クラウド・バイ・デフォルト原則」（2018年） - 政府情報システムは、クラウドサービスの利用を第一候補として検討 - 情報システム化の対象となるサービス・業務、取扱う情報等を明確化した上で、メリット、開発の規模及び経費等を基に検討
クラウド利用の 促進施策 (クラウドサービス 認証制度)	「FedRAMP」（2012年） - 米国連邦政府のクラウドサービス調達のためのリスクおよび認証管理プログラム 2022年1月時点の認証サービス数は247	「G-Cloud framework」（2012年） - 英国政府が運営する、政府機関向けクラウドサービスの調達フレームワーク 2022年1月時点の認証サービス数は38,326	「MTCS SS」（2013年） - シンガポール政府で運用されているセキュリティ管理規格 2022年1月時点の認証サービス数は149	「ISMAP」（2021年） - 政府情報システムのためのセキュリティ評価制度 2022年1月時点の認証サービス数は34
クラウド利用の 促進施策 (情報分類)	- 政府が所有する情報を5段階に分類 - 機密性の低いUNCLASSIFIED／CONTROLLED UNCLASSIFIED INFORMATIONの情報はパブリッククラウドに保管可	- 政府が所有する情報を4段階に分類 - 機密性の低いOFFICIAL／OFFICIAL-SENSITIVEの情報はパブリッククラウドに保管可	-	-

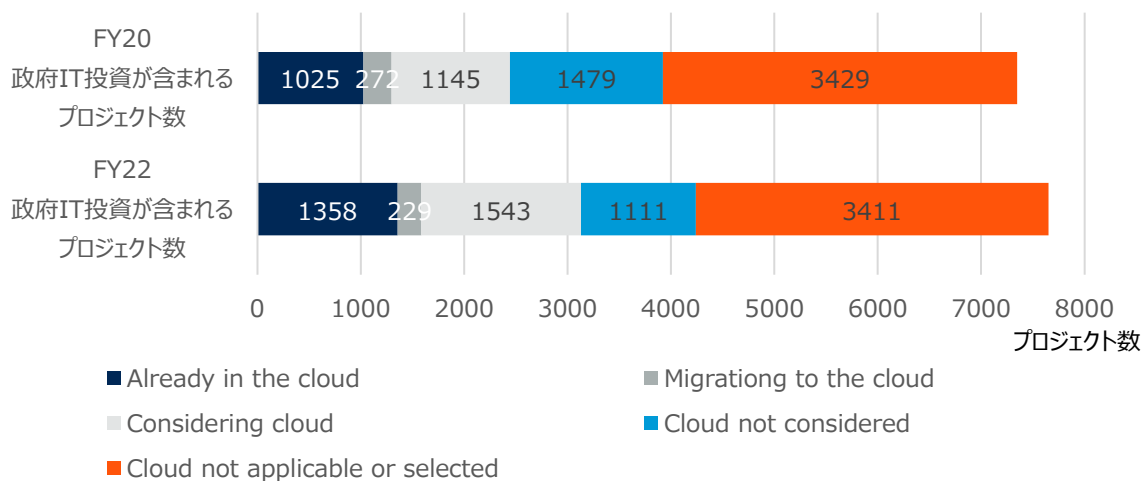
調査c) 各国のクラウドサービス利用状況

政府IT投資が含まれるプロジェクトにおいて、FY22には、20%のプロジェクトでクラウドを既に利用あるいはクラウドへ移行予定、20%のプロジェクトでクラウド利用を検討している。FY20と比較し、クラウドを既に利用・クラウドへ移行予定のプロジェクト数は18%増加している。

クラウドサービス利用割合では、FY18において、パブリッククラウドを利用するシステムが42%と多い。また、ハイブリッドクラウドやコミュニティクラウドの利用も進んでいる

クラウド利用状況

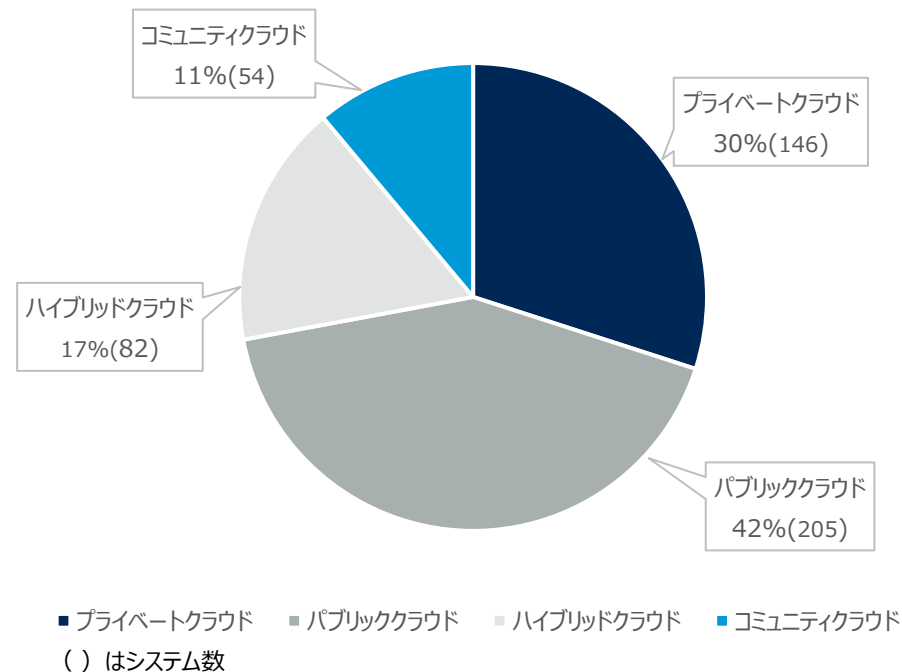
クラウド利用のプロジェクト数（FY22）



出典：有識者ヒアリングをもとに作成

利用サービス

クラウド利用システムにおけるクラウドサービス利用割合（FY18）



出典：GAO Report to Congressional Requesters (April 2019)^{※1}をもとに作成

調査c) 各国のクラウドサービス利用状況 –個別システム事例(1)

米国国防総省の軍輸送システムでは、オンプレミスとパブリッククラウドを組み合わせたハイブリッドクラウドを導入している。可用性の向上やクラウド機能の活用による運用自動化の効果を得ている。また、レガシーアプリケーションのクラウド移行の懸念に対し、アジャイル開発によるアプリケーションの再構築を実施している

政府情報システム	■米国軍輸送システム • 航空、陸上、海上の輸送管理 • ターミナル利用や空中給油を管理
利用しているクラウドサービス	■ハイブリッドクラウド • パブリッククラウドは、IaaSとPaaSを利用
クラウド利用の効果	■可用性の向上、開発容易性、費用対効果 • 障害からの自動復旧 • 復旧時の手動チェックを軽減できたことで数百時間の作業時間を削減 • レポートとトラッキングの仕組みをクラウド機能を組み合わせて自動化し、手動プロセスを排除し貨物輸送情報をほぼリアルタイムで提供 • クラウド利用の価値を最大2,500万ドルと予測
クラウド利用の懸念事項の解決	■レガシーアプリケーションの移行 • 保守が困難であったレガシーアプリケーションをアジャイルの開発手法を取り入れアプリケーションを再構築

出典：GAO Report to Congressional Requesters (April 2019) ※1
 USTRANSCOM News Release ※2

調査c) 各国のクラウドサービス利用状況 –個別システム事例(2)

米国気象システムでは、オンプレミスとパブリッククラウドを組み合わせたハイブリッドクラウドを導入している。コスト削減しながら俊敏性や可用性を向上させ急激なアクセス集中に対応できるようになっている。

政府情報システム	■米国気象システム ・気候／天気／海洋／海岸の変化の状況や予測に関する情報を提供
利用しているクラウドサービス	■ハイブリッドクラウド ・パブリッククラウドは、SaaSを利用
クラウド利用の効果	■コスト削減、俊敏性／可用性を向上 ・急激なアクセス集中時のスケールアップ（通常時は約2,600万／日アクセス、ハリケーンなどの異常気象時は約2億／日アクセス） ・オンデマンドでのスケールアップによるコスト削減 ・利用者にタイムリーな情報を継続的に提供
クラウド利用の懸念事項の解決	—

出典：GAO Report to Congressional Requesters (April 2019) ※1

調査c) 各国のクラウドサービス利用状況 –個別システム事例(3)

米国退役軍人省システムでは、パブリッククラウドに移行している。コスト削減しながら俊敏性、パフォーマンス、可用性を向上させ、また、アプリケーション開発の短縮化を実現している。機密情報を扱うため、サービス事業者が提供する政府向けの専用クラウドサービスを利用している

政府情報システム	■ 米国退役軍人省システム ・ 退役軍人とその扶養家族に患者ケアと連邦給付を提供
利用しているクラウドサービス	■ パブリッククラウド ・ パブリッククラウドは、IaaS（AWS）を利用
クラウド利用の効果	■ コスト削減、俊敏性／パフォーマンス／可用性を向上、開発期間を短縮 ・ サーバをオンデマンドでプロビジョニングすることによるコスト削減 ・ 効率的でモダンなデジタルエクスペリエンス ・ 最新のサービス提供能力 ・ ダウンタイムゼロのメンテナンス ・ 運用の柔軟性の向上 ・ アプリケーション開発や展開サイクルの短縮化
クラウド利用の懸念事項の解決	■ 機密性の高いワークロードを実行するための安全な環境 ・ 患者情報を取り扱うためデータ保護の必要性があり、AWSが米国連邦政府向けに提供する政府専用クラウドサービス（GovCloud）を利用

出典：GAO Report to Congressional Requesters (April 2019) ※1
AWS Public Sector Blog※2

調査c) 各国のクラウドサービス利用状況 – 個別システム事例(4)

英国気象システムでは、オンプレミスとパブリッククラウドを組み合わせたハイブリッドクラウドを導入している。コスト削減をしながら、俊敏性、パフォーマンスおよび拡張性の効果を得ている。また、クラウド人材の確保の懸念に対し、内部に専門家を擁するクラウド運用チームを構成しクラウド運用を実施している

政府情報システム	■ 英国気象システム 気象データを政府、市民、航空、防衛、輸送などの業界に提供
利用しているクラウドサービス	■ ハイブリッドクラウド - パブリッククラウドは、IaaSとPaaS（AWS）を利用 - オンプレミスでは、2台のスーパーコンピューターによる気象モデル分析プログラムを実行 - 機能によるパブリッククラウドとオンプレミスの使い分け
クラウド利用の効果	■ コスト削減、俊敏性／パフォーマンス／拡張性を向上 - 初期設定コストを50%削減 - プロビジョニングを数カ月から数分に短縮 - データ配信を数分から数秒に高速化 - テストは数カ月から24時間で完了 - ストレージをオンプレミスでは50%拡張が未サポートの状況から1,000%拡張
クラウド利用の懸念事項の解決	■ クラウド人材の確保 インハウスによる多くの専門家を擁するクラウド運用チームを構成

出典：AWS Case Study ※1

調査c) 各国のクラウドサービス利用状況 – 個別システム事例(5)

英国運転免許システムでは、オンプレミスとパブリッククラウドを組み合わせたハイブリッドクラウドを導入している。コスト削減をしながら、拡張性、弾力性、俊敏性、および柔軟性の効果を得ている。また、クラウドに対応したアプリケーションアーキテクチャやレガシーシステムとの接続の懸念に対し、マイクロサービス化およびAPI経由での接続を実現している

政府情報システム	▪ 英国運転免許システム • 4,700万人以上の運転者記録を保持し、運転免許証の発行や自動車税の納税を管理（月間7,000万以上のアクセス）
利用しているクラウドサービス	▪ ハイブリッドクラウド • パブリッククラウドは、PaaS（AWS）を利用 • オンプレミスでは、個人情報等の機密情報を管理 • 情報種別によるパブリッククラウドとオンプレミスの使い分け
クラウド利用の効果	▪ コスト削減、拡張性／弾力性／俊敏性／柔軟性を向上 • 月間数十億トランザクションをサポートする大規模な拡張性 • 大きく変動する需要に対応するための弾力的なスケーリング • サーバレスコンピューティングによるコスト削減と俊敏性の向上 • ハイブリッドアーキテクチャをサポートするためにトランザクション量を調整する柔軟性
クラウド利用の懸念事項の解決	▪ レガシーシステムのクラウド移行、レガシーシステムとの接続 • アプリケーションをマイクロサービスに分解し、コンポーネントごとに最も適切なテクノロジーやサービスを選択 • API経由でオンプレミスのシステムと接続 • 開発経験が豊富な外部ベンダーとの提携

出典：AWS Case Study ※1
Digital Leaders article ※2

調査c) 各国のクラウドサービス利用状況 – 個別システム事例(6)

英国労働年金システムでは、オンプレミスと複数のパブリッククラウドを組み合わせたマルチクラウドを導入している。可用性、柔軟性および拡張性の効果を得ている。また、クラウド人材の確保の懸念についてはHPE社よりスタッフを採用、クラウドに対応したアプリケーションアーキテクチャやレガシーシステムとの接続の懸念に対し、マイクロサービス化およびAPI経由での接続を実現している

政府情報システム	■英国労働年金システム • 福祉、年金、養育費等の給付を管理
利用しているクラウドサービス	■マルチクラウド／ハイブリッドクラウド • パブリッククラウドは、AWSとAzureを利用 • オンプレミスでは、個人情報等の機密情報を管理 • 情報種別によるパブリッククラウドとオンプレミスの使い分け
クラウド利用の効果	■可用性／柔軟性／拡張性を向上
クラウド利用の懸念事項の解決	■クラウド人材の確保 • ヒューレットパカードエンタープライズから約400人のスタッフを採用 ■レガシーシステムのクラウド移行、レガシーシステムとの接続 • アプリケーションをマイクロサービスに分解し、コンポーネントごとに最も適切なテクノロジーやサービスを選択 • API経由でオンプレミスのシステムと接続

出典：Computer Weekly article ※1※2

調査c) 各国のクラウドサービス利用状況 - 政府専用クラウドサービス

大手サービス事業者は、米国連邦政府向けに機密性の高い情報を扱うことができる政府専用クラウドサービスを提供している。本調査時点では、米国のみでの提供となっている

- **AWSとMicrosoftは米国連邦政府向けに機密情報や規制対象のワークロードを動かすことができる政府専用クラウドサービスを提供**

AWS GovCloud (US)

- AWS GovCloud (US-East)
 - 3 Availability Zones
- AWS GovCloud (US-West)
 - 3 Availability Zones

Azure Government

- 3 US Gov Regions
- 2 US DoD Regions
- 3 US Sec Regions
 - Note: only 1 (US Gov Virginia) has multiple Availability zones

特徴

- 米国内の物理的に隔離されたデータセンター、データ主権を保証
- 従業員は全員米国籍
- 米国政府機関および政府規制下の産業における組織からのアクセスに制限、ルートアカウント保持者は米国市民であることを確認する必要がある
- 商用クラウドのサービスとは若干異なり、主にセキュリティオプションに制約があり費用も高い
- 特定の政府機関向けに特化した専用クラウドサービスも提供
 - 政府系情報機関（IC、Intelligent Community）向けとして、AWSは物理的に独立したインスタンスを提供し、ICが管理運用する「Unclassified」、「Sensitive」、「Secret」、「Top Secret」の全てのレベルの情報を取り扱うことが可能
 - 国防総省向けとして、Microsoftが単一ベンダーで専用クラウドを構築しようとしたが断念し、マルチベンダー戦略で再検討中

出典：有識者ヒアリングをもとに作成

『他国政府のクラウド利用の調査』の全体総括（1/3）

各国政府はクラウド利用推進の方針のもと政府情報システムへのクラウド利用を進めている。また、クラウド利用推進の方針を支援するため、クラウドを安心安全に利用するためのガイドラインや基準を統一化し、セキュリティ認定制度を設立・クラウドサービスの認定を進めている。また、保持する情報を分類し、機密性の低い情報はパブリッククラウドに保存することを承認している

	調査内容	調査サマリ
a) 他国政府におけるクラウドサービスの利用方針	他国政府におけるクラウドサービスの利用方針やガイドライン等について、各国特有の事情や背景を踏まえた特徴や違いを調査する	デジタル政府戦略を推進する各国は、政府イニシアチブによる政府情報システムへのクラウド利用を促進 ■ 米国や英国は、2010年以降、早期に政府が「クラウド・ファースト戦略」を掲げ、クラウドを優先的に利用する原則のもと、クラウド利用を拡大 ■ シンガポールは、英国等の他国の事例を参考に、政府情報システムの大半をパブリッククラウドへ移行する計画のもと、クラウド利用を拡大
b) 各国のクラウドサービス利用の促進施策	各国におけるクラウド利用を促進する施策・制度・仕組み等について、各国特有の事情や背景を踏まえた特徴や違いを調査する	クラウドサービスを統一基準で評価する認定制度を導入し、調達効率性を向上 ■ 各国のセキュリティ認定制度として、FedRAMP（米国）、G-Cloud Framework（英国）、MTCS SS（シンガポール）がある。各国の省庁等の政府機関は原則としてセキュリティ認定を受けたクラウドサービスを調達 ■ 運用開始後、認証までの期間と高コストが問題視され、認証申請プロセスを効率化し、期間短縮やコスト低減を実現する取り組みが継続的に行われている 政府が所有する情報を機密性や重要性の観点から分類しパブリッククラウドに保存できる情報分類を定義 ■ 米国や英国では、政府の所有する情報を分類しパブリッククラウドに保管できる定義している。米国の例では、機密性の低いUNCLASSIFIED／CONTROLLED UNCLASSIFIED INFORMATIONの情報はパブリッククラウドに保管可としている クラウド利用の戦略を導入後、戦略のレビューを行い、セキュリティ、調達、人材等に関する課題に対応するため戦略の見直しを実施 ■ 米国では、クラウドサービス利用前にその必要性の評価が必要としている「クラウド・スマート戦略」を導入。英国では、セキュリティ、調達、人材等の課題に対するガイダンスや事例を記したクラウド活用ガイド（The One Government Cloud Strategy）を発表

『他国政府のクラウド利用の調査』の全体総括（2/3）

各政府は、ハイブリッドクラウドの採用やクラウド人材の確保などの施策によりクラウド利用の懸念を解消し、クラウド利用を拡大している。大手サービス事業者が機密性の高い情報を管理できる政府専用クラウドサービスを提供している事例もある

c) 各国のクラウドサービス 利用状況

調査内容

各国における政府系システムのクラウドへの移行状況などの概況とその背景・理由などを調査する

調査サマリ

機密性の低い情報を扱うシステムや、経済性や俊敏性等のクラウド利用のメリットを享受できることが明確なシステムを中心にクラウド利用が拡大

- 米国では20%のITプロジェクトでクラウドを利用、20%のITプロジェクトでクラウド利用を検討。パブリッククラウドやプライベートクラウドを利用するプロジェクトが多い
- 政府情報システムのうち、英国では約60%、シンガポールでは約70%のシステムでパブリッククラウドを利用※1
- コストを削減しながら、拡張性・弾力性、俊敏性、柔軟性等の向上させている事例が多い

機密性の高い情報管理や人材不足などのクラウド利用の懸念に対し、ハイブリッドクラウドの利用やクラウド有識者を採用するなど解決策を実施

- クラウドの利用形態として、ハイブリッドクラウドが機密性の高い情報を管理する場合の代表的なユースケースとなっている
- クラウド人材確保の懸念について、クラウド移行や運用の経験豊富なパートナーとの連携、ベンダーからクラウド有識者を大量採用している事例がある

大手サービス事業者による政府の機密性の高い情報を管理できる政府専用クラウドサービスの提供

- 米国ではAWSやMicrosoftが提供する機密性の高い情報を扱うことができる政府専用クラウドサービスを提供し、政府機関での利用が進みつつある

『他国政府のクラウド利用の調査』の全体総括（3/3）

他国政府のクラウドサービスの利用方針・利用促進施策・利用状況をふまえると、日本における政府情報システムのクラウド利用を促進するためには、クラウド利用の課題に対するガイダンス提供、クラウドサービスのセキュリティ認定取得のプロセス簡素化、機密性の高い情報を管理できる専用クラウドサービスの開発が望まれる

日本において考慮すべき事項

クラウド利用の課題に対するガイダンスの提供

- 日本においては、「クラウド・バイ・デフォルト原則」のもと、政府によるクラウド利用を促進している。今後は、クラウド利用を進める中で政府機関が直面しがちな課題を抽出し、ガイダンスや事例の追加や更新を先行して実施していくことが重要となる。セキュリティ、調達、および人材の3つの領域の重要性を認識し、ガイダンス提供の準備を進めている米国の例は参考になると考えられる

セキュリティ認定取得のプロセス簡素化

- クラウド利用の促進において、利用できるクラウドサービスを増やしていくことも重要となる。日本のセキュリティ認定制度（ISMAP）においても、審査の費用低減や期間短縮に向け、クラウドサービスのリスクに応じた審査項目の設定や、審査の自動化などが進むと考えられる

機密性の高い情報を管理できる専用クラウドサービスの開発

- サービス事業者と連携し、政府が保持する機密性の高い情報をクラウド上で管理可能な専用クラウドサービスを開発および利用することで、クラウド利用が拡大すると想定される
- 米米国での大手サービス事業者の例を鑑みると、政府専用クラウドサービスの開発にあたっては、日本国内の専用データセンターを利用していること、機密性の高い情報を管理するための高度なセキュリティ対策を実施していること、クラウドサービスの提供実績が多いこと、日本の法規制を遵守できること等を踏まえた上でベンダーを選定し、連携することが重要であると考えられる

4. 重要情報を取り扱う企業等におけるクラウドサービスの利用実態・懸念点

クラウドサービスの利用実態・懸念点：調査項目

クラウド利用に関する実態・懸念点調査では、企業へのアンケート調査・ヒアリング調査およびクラウドサービス事業者へのヒアリング調査によって、クラウドサービスの利用実態やクラウドサービスの利用拡大にあたっての懸念と期待等を明らかにする

項目	調査内容	調査方法
重要情報を取り扱う企業等におけるクラウドサービスの利用実態・懸念点	クラウドサービスの利用実態 - どのような業務領域について、どのようなクラウドサービスを利用しているか - クラウドサービス利用に関する戦略・方針はあるか - クラウドサービスを積極利用している企業の特徴は クラウドサービスの利用目的・享受しているメリット - どのような目的のもとクラウドサービスを利用しているか（業務変革スピード、コスト削減、セキュリティ、クラウド技術の利用、等） - クラウドサービス利用によってどのようなメリットを享受しているか クラウドサービスの利用にあたっての懸念 - クラウドサービスの利用拡大に向け、どのような懸念点・課題があるか - 信頼性・安定性（災害対策・可用性、応答時間・超低遅延、セキュリティ、等） - 利便性・機能性（オープン性、運用のしやすさ、柔軟性、機能の多さ、等） - その他（ベンダーロックイン、国内法の適用、企業の持続可能性、環境負荷、等） - クラウドサービス利用に伴い、採用しているテクノロジーや取っている対策はどのようなものか 期待される技術や制度 - クラウドサービスの利用拡大にあたり期待される技術は - クラウドサービスの利用拡大にあたり期待される制度は - 政府やクラウドサービス事業者期待することは何か	- 企業へのアンケート調査 - 企業へのヒアリング調査 - クラウドサービス事業者へのヒアリング調査

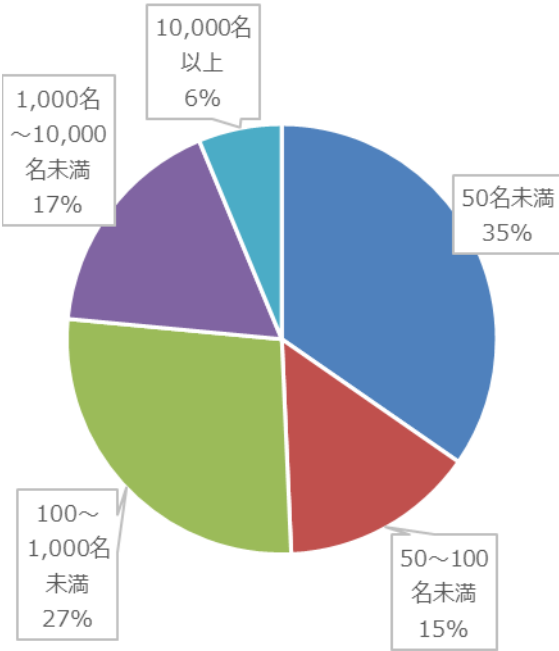
アンケート調査実施概要

重要インフラ産業を中心に、令和4年2月にWebアンケート調査を実施。有効回答数430件

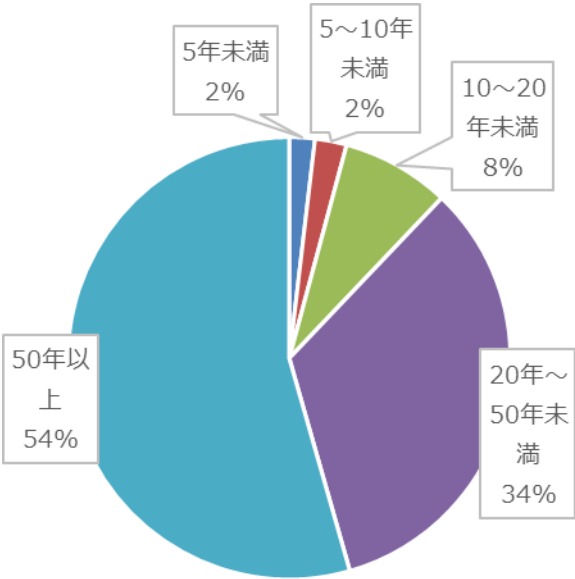
調査対象業種一覧

業種大分類	業種
金融	銀行 クレジット
運輸・輸送	物流 鉄道 航空（回答者無し） 空港（回答者無し）
規制インフラ	情報通信 電力 ガス
化学	化学 石油（回答者無し）
医療	医療
その他	自動車 鉄鋼 熱供給 その他

回答企業従業員数



回答企業創業年数



ヒアリング調査実施概要

重要インフラ産業を中心に、主にクラウド利用を積極的に行っていると思われる企業10社を対象にヒアリング調査を実施

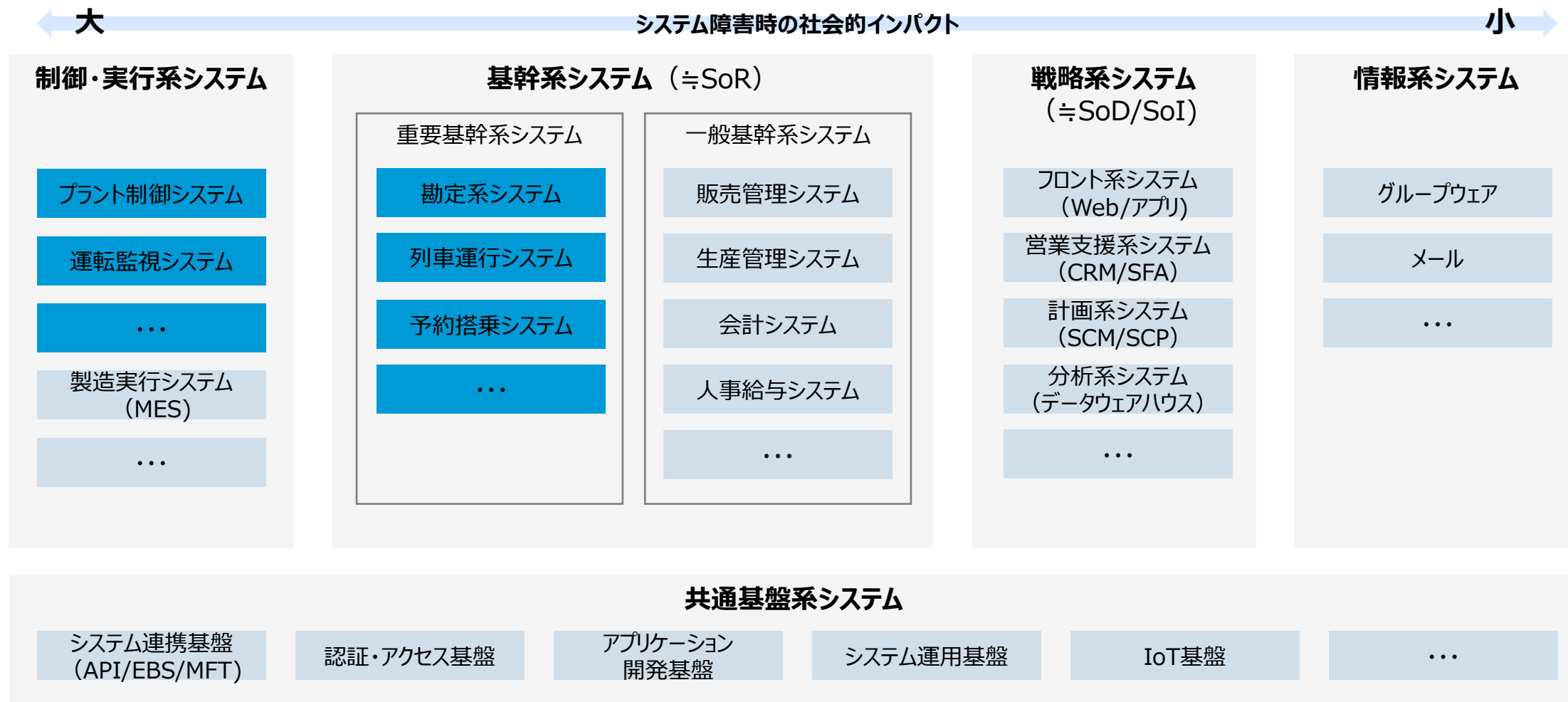
		(重要システムのシステム利用環境)							
		業種大分類	従業員数	クラウド利用方針	オンプレミス 単一利用	プライベートクラウド 単一利用	パブリッククラウド 単一利用	ハイブリッドクラウド 利用	マルチクラウド 利用
1	A社	金融	10,000名以上	クラウド優先	○			○	○
2	B社	運輸・輸送	10,000名以上	クラウド優先	○	○	○	○	○
3	C社	運輸・輸送	10,000名以上	オンプレミス優先	○	○		○	
4	D社	規制インフラ	1,000～10,000名 未満	クラウド優先	○		○	○	
5	E社	規制インフラ	10,000名以上	クラウド優先	○	○	○		○
6	F社	化学	1,000～10,000名 未満	オンプレミス・プライベートクラウド優先	○	○		○	
7	G社	化学	10,000名以上	クラウド優先	○	○	○	○	○
8	H社	医療	100～1,000名未満	クラウド優先		○		○	
9	I社	医療	1,000～10,000名 未満	オンプレミス優先	○			○	
10	J社	その他 (製造業)	10,000名以上	クラウド優先	○	○	○	○	○

調査対象システムの分類

重要システム

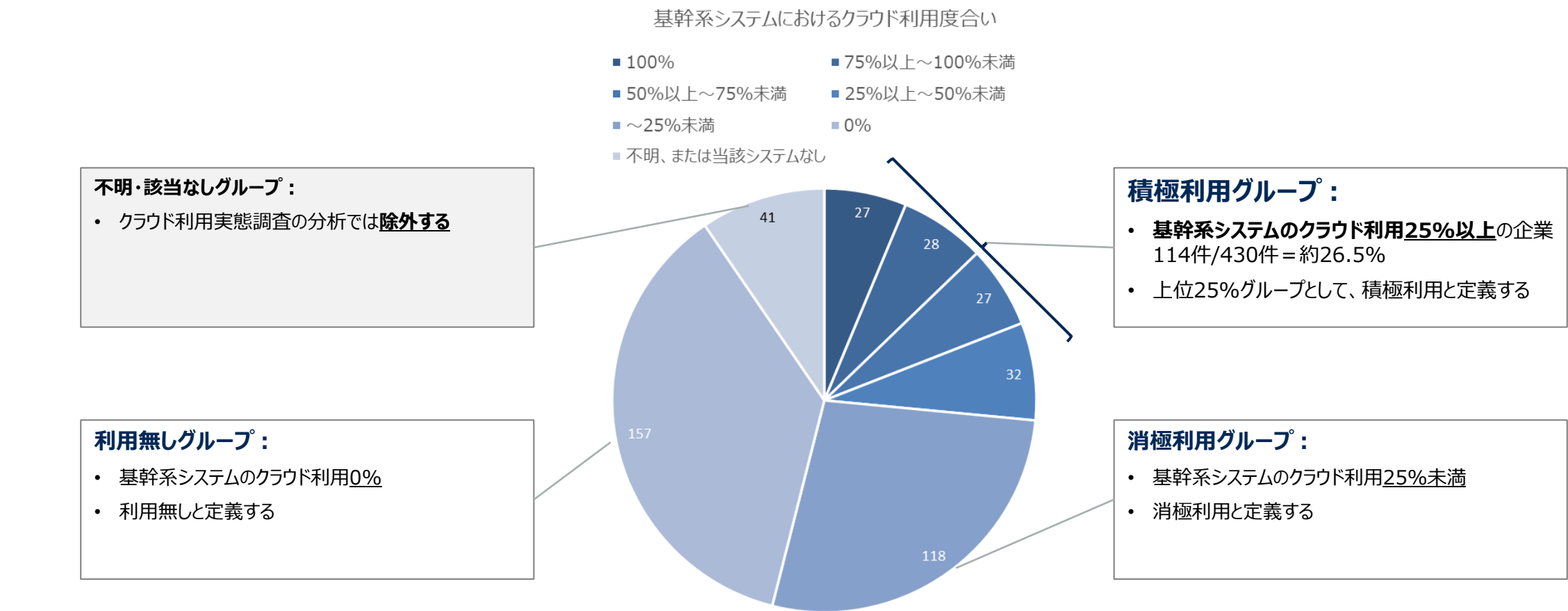
通常システム

重要インフラ企業においても様々なシステムが存在し、その重要度によってクラウドの利活用の度外が大きく異なると想定。今回は以下の5つの分類でのクラウド活用の概観を捉えつつ、特にクラウド活用が進んでいないと想定される「重要システム」について、利用実態を把握する



クラウド積極利用・消極利用グループの定義

5つのシステム系列の中でも重要な基幹系システムにおいて、クラウド利用率が全サンプルの上位25%に当てはまるのは、利用率25%～100%の企業。それらを積極利用グループとし、25%未満を消極利用グループ、0%を利用無しグループに分けて、比較分析を行った



クラウドサービスの利用実態：調査結果サマリ

情報系システムではクラウド利用が進んでいる一方、制御・実行系システムへのクラウド利用は進んでいない。クラウド・ファーストポリシーを持っている企業であっても、必ずしも組織全体がクラウド化への理解や意識が一帯ではなく、重要システムにおいてはクラウド化に慎重な姿勢が強い

どのような**業務領域**について、どのようなクラウドサービスを利用しているか？

どのように**使い分け**しているか？

情報系システムではクラウド利用が進んでいる一方、制御・実行系システムへのクラウド利用は進んでいない

- クラウド利用が進んでいるシステムは情報系システムがトップ、次いで基幹系システム。制御・実行システムのクラウド化はほとんど進んでいない [アンケート調査]

システムの重要性や情報の機密性によってオンプレミス・プライベートクラウドとパブリッククラウドを使い分けている

- システムの重要性による使い分け [G社、H社、F社]、情報の機密性による使い分け [B社、C社、D社、I社]、パブリッククラウドへの移行期のため結果的に使い分け [A社、E社]

クラウド利用が積極的な企業ほど、ハイブリッドクラウドやマルチクラウドの利用率が高い

- 回答企業の2割がハイブリッドクラウドを、1割弱がマルチクラウドを利用していると回答 [アンケート調査]
- ハイブリッドクラウドは、認証基盤との連携、重要情報を保存しているシステムとの連携などで利用
 - オンプレミスの認証基盤との連携 [C社、H社]、重要情報を保存しているオンプレミスのシステムとの連携 [C社、D社、F社、H社、I社]

コストメリット等の観点から特定クラウドベンダーへ集約しつつ、一部用途によっては複数ベンダーを使い分けている

- 戦略的に特定クラウドベンダーに集約しつつ、機械学習などは他のクラウドベンダーを利用 [B社]、ボリュームディスカウント等の観点から特定クラウドベンダーに集約、但し特定クラウドベンダー固有の機能が必要な場合は他のクラウドベンダーを利用 [E社]

クラウドサービス利用に関する**戦略・方針**はあるか？
クラウドサービス利用が進んでいる**企業の特徴**は？

クラウド・ファーストのポリシーのもとクラウド利用を推進しているも、重要システムへの適用は慎重な姿勢が強い

- クラウド・ファーストのポリシーを掲げクラウド利用を推進している企業には下記の特徴がある
 - クラウド化のメリットを享受するため、利用するクラウドサービスの優先度（SaaS、PaaS、IaaSの順）を設定している [A社、B社、D社、E社、G社]
 - 数年前からクラウド・ファーストのポリシーのもとクラウド利用を推進しているため、現時点でのクラウド利用は低いが、今後のシステム更改にあわせてクラウド利用が拡大していくと想定される [A社、B社、D社、E社、G社、J社]
- 工場等の制御・実行系システムなどの一部の重要システムでは、業務部門主導でシステム構築しクラウド化の検討自体も業務部門に委ねている企業が多い [C社、D社、E社、J社]。当該システムについては、クラウド化の検討の優先度を下げる、クラウド化の対象外としてオンプレミスのままとする、といった方針としている [C社、D社、E社、G社、J社]

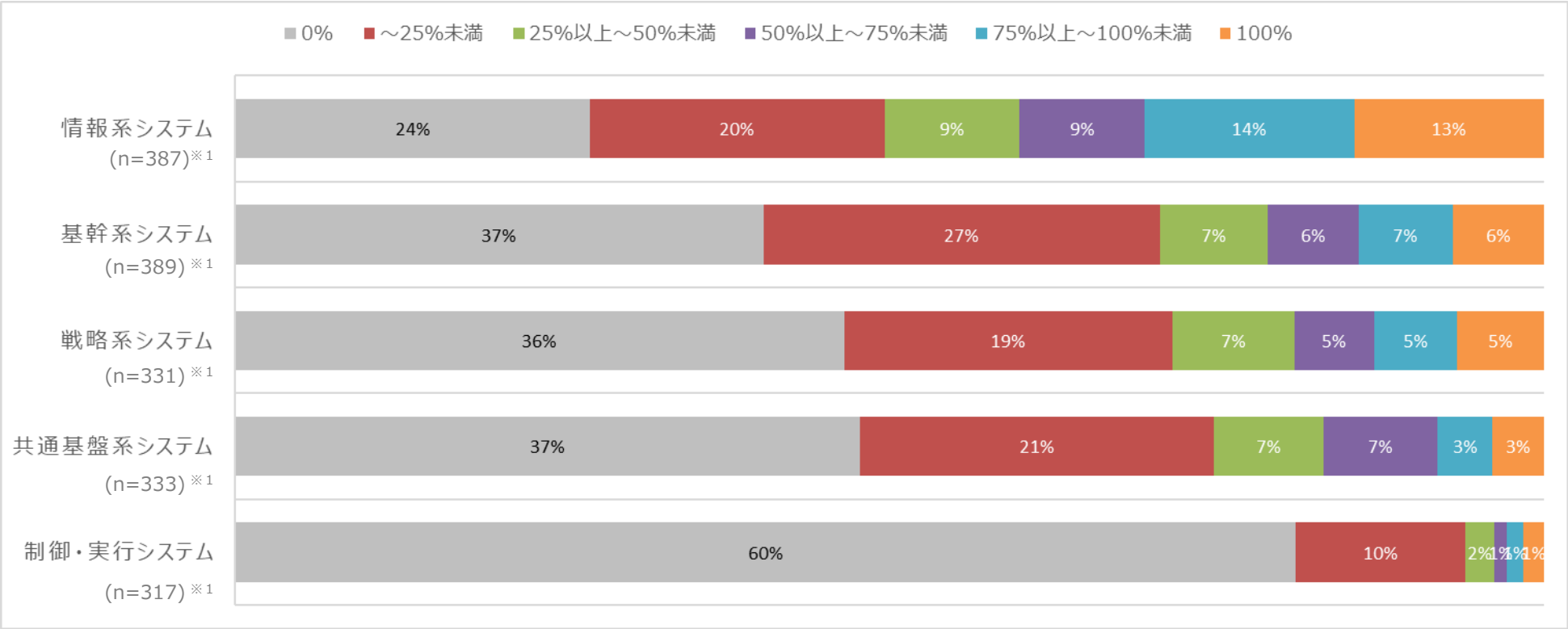
クラウド利用が進んでいる企業は経営がイニシアチブを持って推進している

- 経営層・ビジネス部門のリーダーがクラウドが必要という意識を持つと、クラウド利用の戦略・方針が明確なものとなり、クラウドをどう活用するかという意識で組織全体が進む。進んでいる企業は、クラウド利用のガイドラインが整備されており、ここまで使ってよいという線引きが明確。更に利用が進むにつれてそのバーを上げていく [クラウド事業者ヒアリング]
- 一方で、多くの企業では、「クラウドファースト＝クラウドを使っても良い」となっており、なぜクラウドを使わないといけいないのか、これまでの方法の方が安心、という意識になり、結果的にクラウドを選択しないことが多い。保守的な企業は、ルールを作る際に保守的になり、かえってクラウドを使いにくくしている。また、現場が理解が高くても、中間管理職がクラウドをよく理解しておらず、経営層に説明出来ず、クラウド導入に至らないこともある [クラウド事業者ヒアリング]

アンケート調査結果：クラウドサービスの利用状況

クラウド利用が進んでいるシステムは情報系システムがトップ、次いで基幹系システム。制御・実行システムのクラウド化はほとんど進んでいない

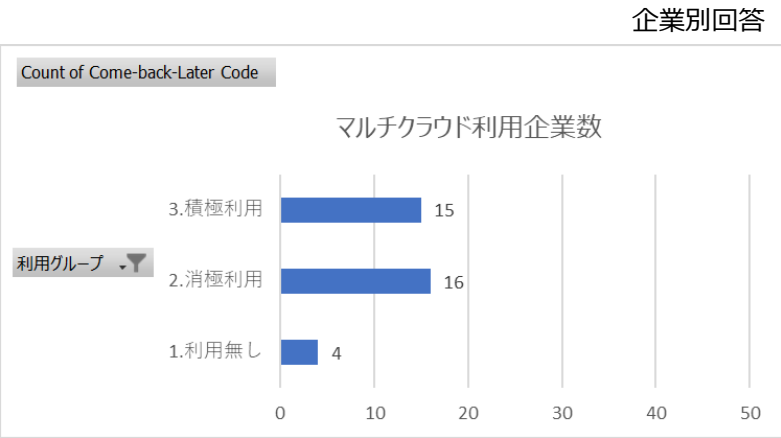
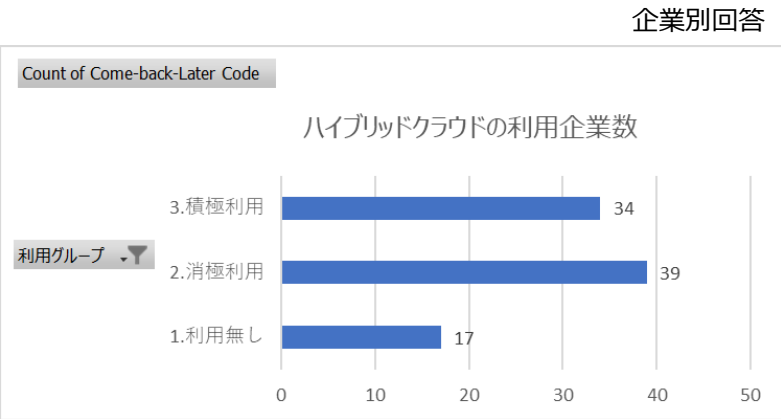
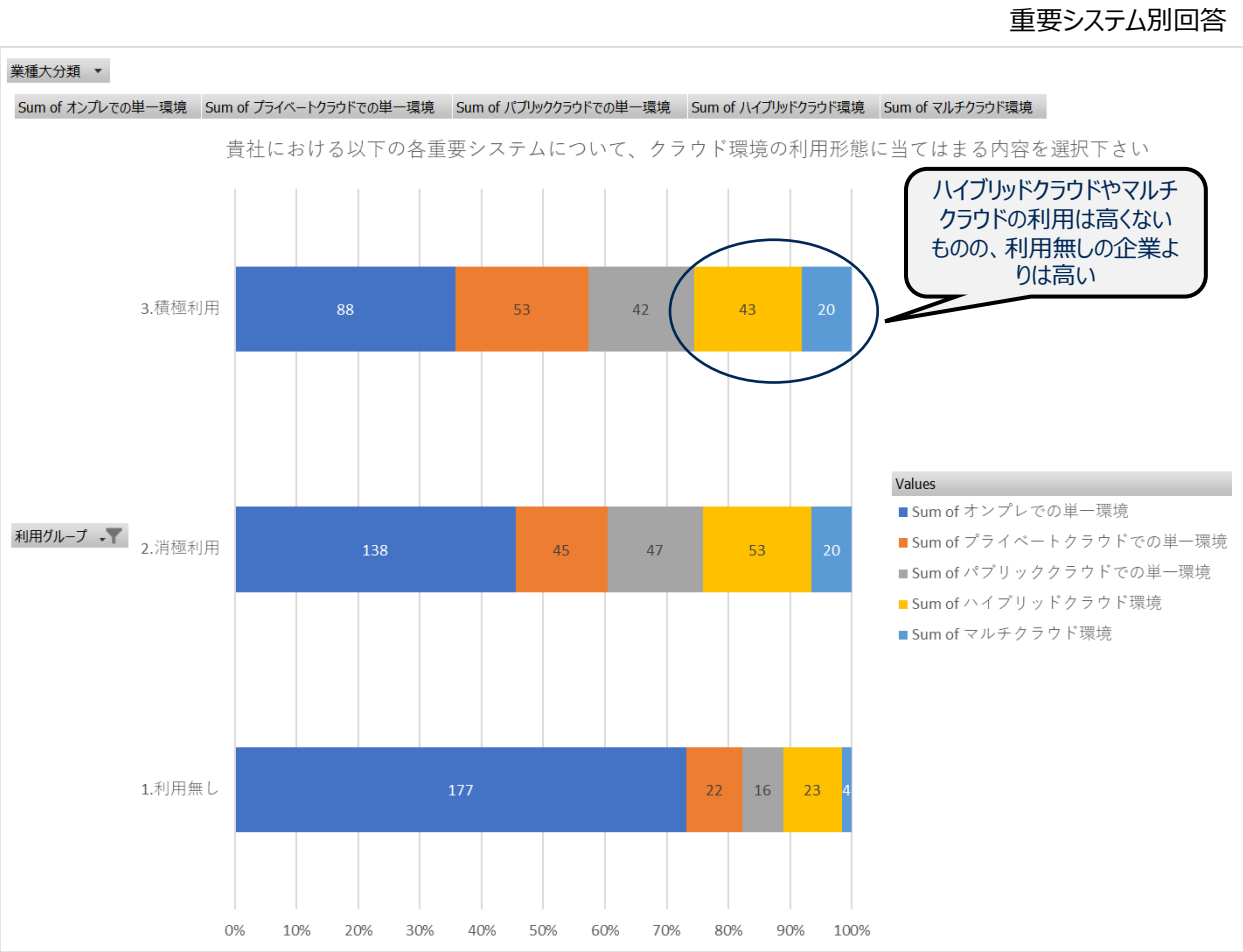
貴社におけるシステムについて、クラウドの利用度合いについて回答下さい



※ 1 回答企業数（但し、「不明、または当該システムなし」と回答した企業を除く）

アンケート調査結果：ハイブリッドクラウド・マルチクラウド利用実態

ハイブリッドクラウドやマルチクラウドの利用率は高くはないものの、積極利用の企業は、利用の無い企業と比べ、利用率が高い



回答企業数

金融： n=140
運輸・輸送： n=17
規制インフラ： n=127
化学： n=33
医療： n=19
その他： n=94

重要システム数

クレジット： 2
銀行： 12
鉄道： 4
物流： 4
ガス： 3
電力： 3
情報通信： 4
化学： 2
医療： 2
その他： 1
自動車： 1
鉄鋼： 1
熱供給： 1

※利用無し＝基幹系システムにおけるクラウド利用が0%と回答した企業
※消極利用＝基幹系システムにおけるクラウド利用が25%未満と回答した企業
※積極利用＝基幹系システムにおけるクラウド利用が25%以上と回答した企業

クラウド導入の理由/享受しているメリット：調査結果サマリ

セキュリティ、業務改革スピードやコスト削減が主なクラウドの導入理由として挙げられた。クラウドの高いセキュリティレベルはメリットという理解があり、また事業や社会の変化に追いつくためにクラウドが活用されている

クラウドサービス利用によってどのような**メリット**を享受しているか？

クラウドの高いセキュリティレベルはメリットとして捉えられている

- セキュリティはクラウド利用で最も重視する導入理由。規制の厳しい金融・規制インフラ業種ではセキュリティを重視。規制インフラ・その他ではセキュアなデータ管理の利便性、金融・化学では導入構築における自社負担軽減の利便性を感じている [アンケート調査]
- クラウド利用におけるセキュリティのメリットとして、クラウド事業の高度なセキュリティ対策をあげている
 - クラウド事業者のセキュリティ対策を理解した上でセキュリティをメリットとしてあげている [B社、C社、E社、G社、J社]
 - クラウド事業者を信頼しセキュリティに関する問題が発生することは考えていない [H社、I社]
- 既存システムにおいてセキュリティ対策としてクラウド事業者と同様レベルの投資や対策を実施していることから、セキュリティのメリットはない [A社]

事業変化に迅速に対応するためクラウドを利用

- 業務改革スピードは、セキュリティに次ぐクラウド利用で重視する事項。既存外部サービスの修正・変更や、新規自社開発サービス導入のスピードの利便性を高く感じている [アンケート調査]
- 事業環境の変化による競争激化の伴い短期間でのシステム開発・サービス提供が求められる
 - 1年かかる開発を4か月に短縮し年2回のタイミングで新規サービスをマーケットイン、利用状況に応じて直ぐに撤退 [A社]、3か月かかる開発1か月に短縮 [E社]、業務部門からの短納期での環境用意への要望に対応 [C社、F社、G社、J社]、クラウド導入することで業務改革のスピードが今後上がることを期待している [I社]
- ユースケースとして多いのは、業務改革、デジタルサービス開発。近年はコロナやリモートワークなど、社会の変化に応じた緊急の活用の影響もある [クラウド事業者ヒアリング]

クラウドはIT投資額の削減に効果

- コスト面では、多くの業種で初期投資額の削減メリットを得られている [アンケート調査]
- コスト削減の対象として、初期構築費用の削減、既存サーバの運用保守費用の削減をあげている [C社、D社、E社、G社]
- 自前のシステムがあり内製メンバーで運用できていることからクラウド化がコスト削減につながらないと捉えている [J社]
- コスト削減もドライバの一つ。金融機関で初期のころ典型的だったのは、コストのかかるリスク計算 [クラウド事業者ヒアリング]

業務変革スピードやコスト削減を実現する拡張性

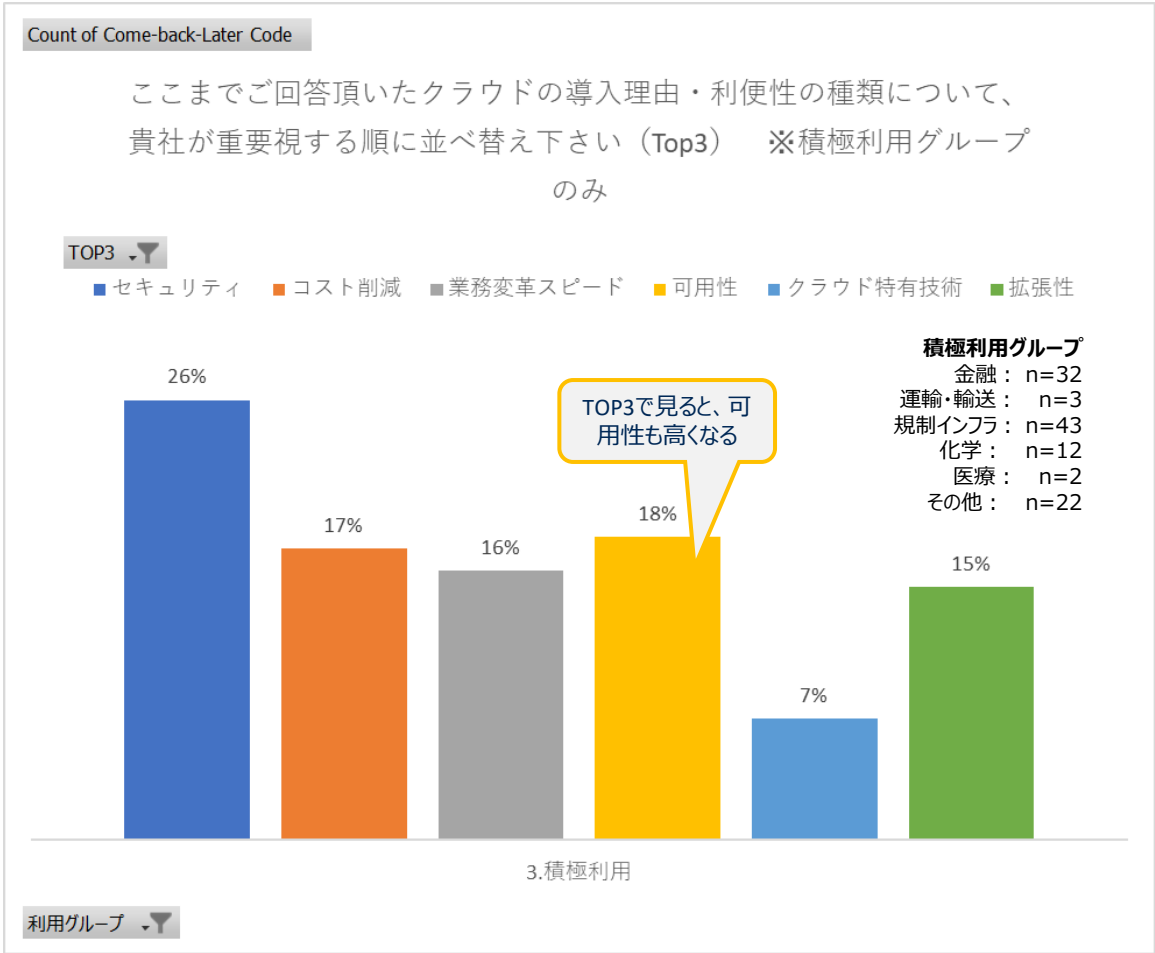
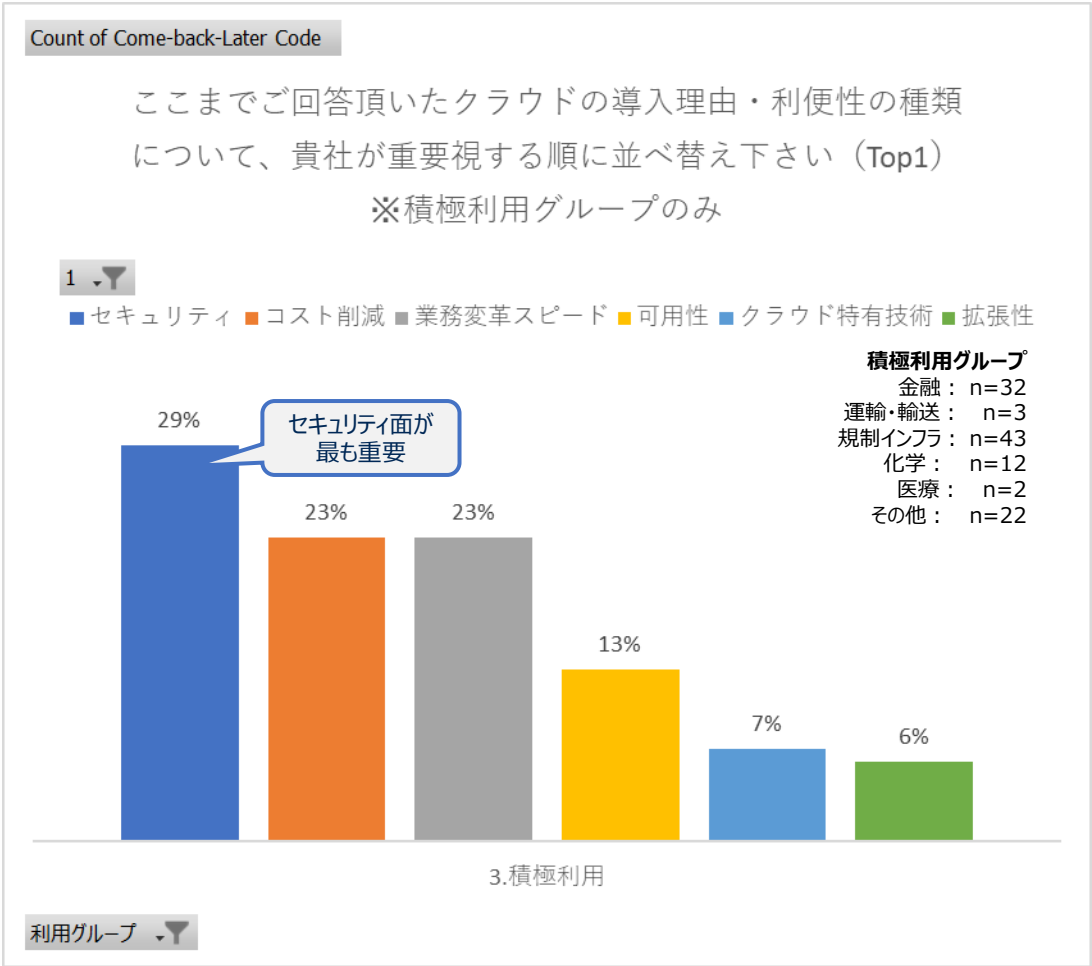
- 可用性、拡張性、クラウド特有技術を挙げる企業はそれぞれ全体の1割程度のみ [アンケート調査]
- 業務変革スピードやコスト削減をあげているがこれらを実現するために拡張性が最も重要としている [A社]

AI・データ分析のクラウド特有技術の活用のためにクラウドを利用

- モノからサービスへビジネスを進化させるにあたって必要となるAI・データ分析の能力をクラウドから享受している [G社]

アンケート結果：積極利用企業 クラウドの導入理由 Top1/Top3

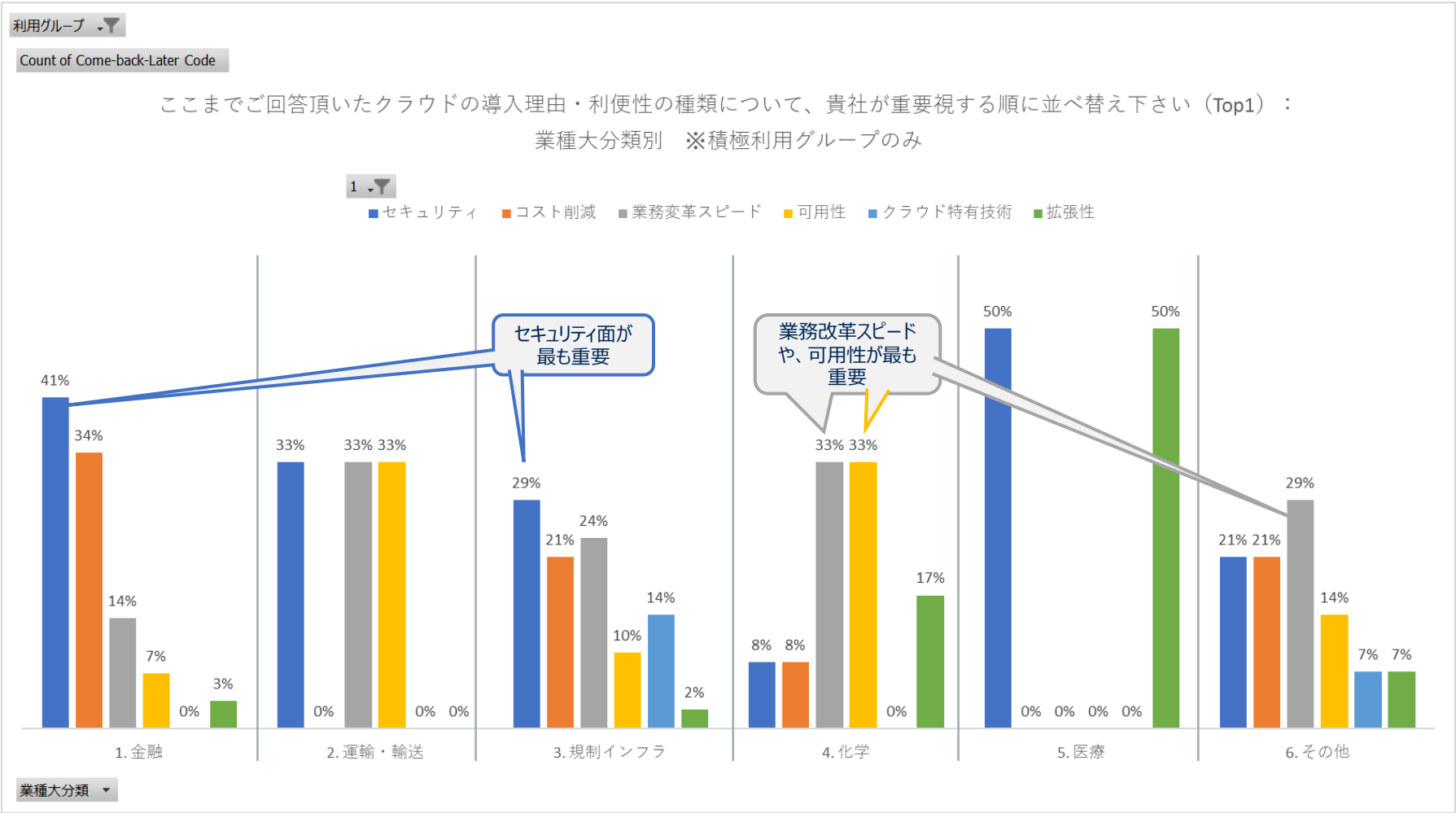
セキュリティ面が最も重要。次いで業務改革スピードとコスト削減。積極利用の企業は、オンプレよりもクラウドの方がセキュアであるという認識を持っているといえる。TOP3で見ると、可用性も高くなる



※利用無し＝基幹系システムにおけるクラウド利用が0%と回答した企業
※消極利用＝基幹系システムにおけるクラウド利用が25%未満と回答した企業
※積極利用＝基幹系システムにおけるクラウド利用が25%以上と回答した企業

アンケート結果：積極利用企業 クラウドの導入理由Top1（業種別）

規制の厳しい金融・規制インフラではセキュリティを重視。化学・その他業種では業務改革スピードや可用性を重視している



積極利用グループ

金融： n=32
運輸・輸送： n=3
規制インフラ： n=43
化学： n=12
医療： n=2
その他： n=22

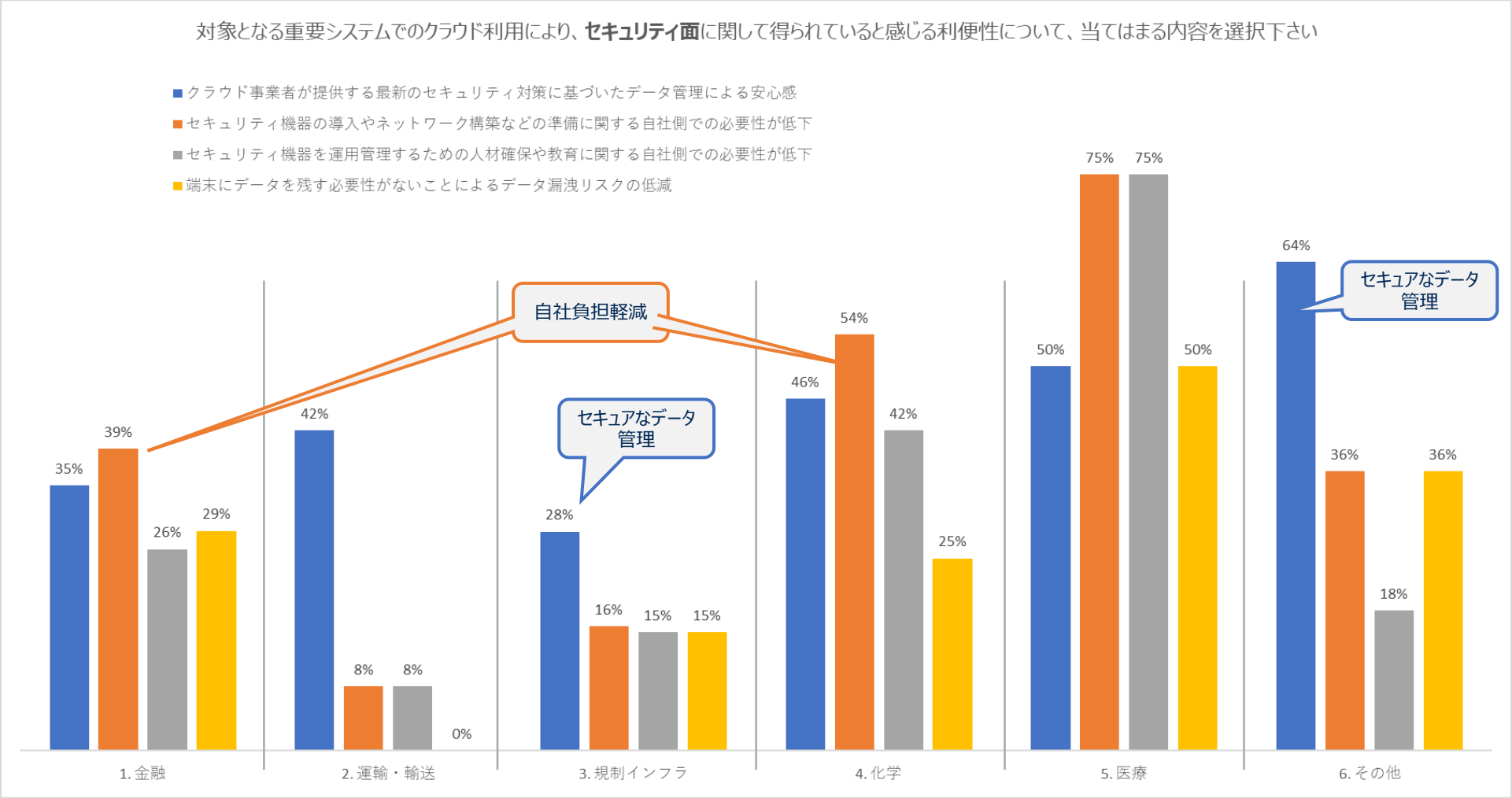
重要システム数

クレジット： 2
銀行： 12
鉄道： 4
物流： 4
ガス： 3
電力： 3
情報通信： 4
化学： 2
医療： 2
その他： 1
自動車： 1
鉄鋼： 1
熱供給： 1

※「2.運輸・輸送」および「5.医療」の積極利用グループ企業はn数が少ない為、回答結果には留意が必要

アンケート結果：積極利用企業 セキュリティ面で得られている利便性

規制インフラ・その他ではセキュアなデータ管理の利便性、金融・化学では導入構築における自社負担軽減の利便性を感じている



積極利用グループ

金融： n=32
運輸・輸送： n=3
規制インフラ： n=43
化学： n=12
医療： n=2
その他： n=22

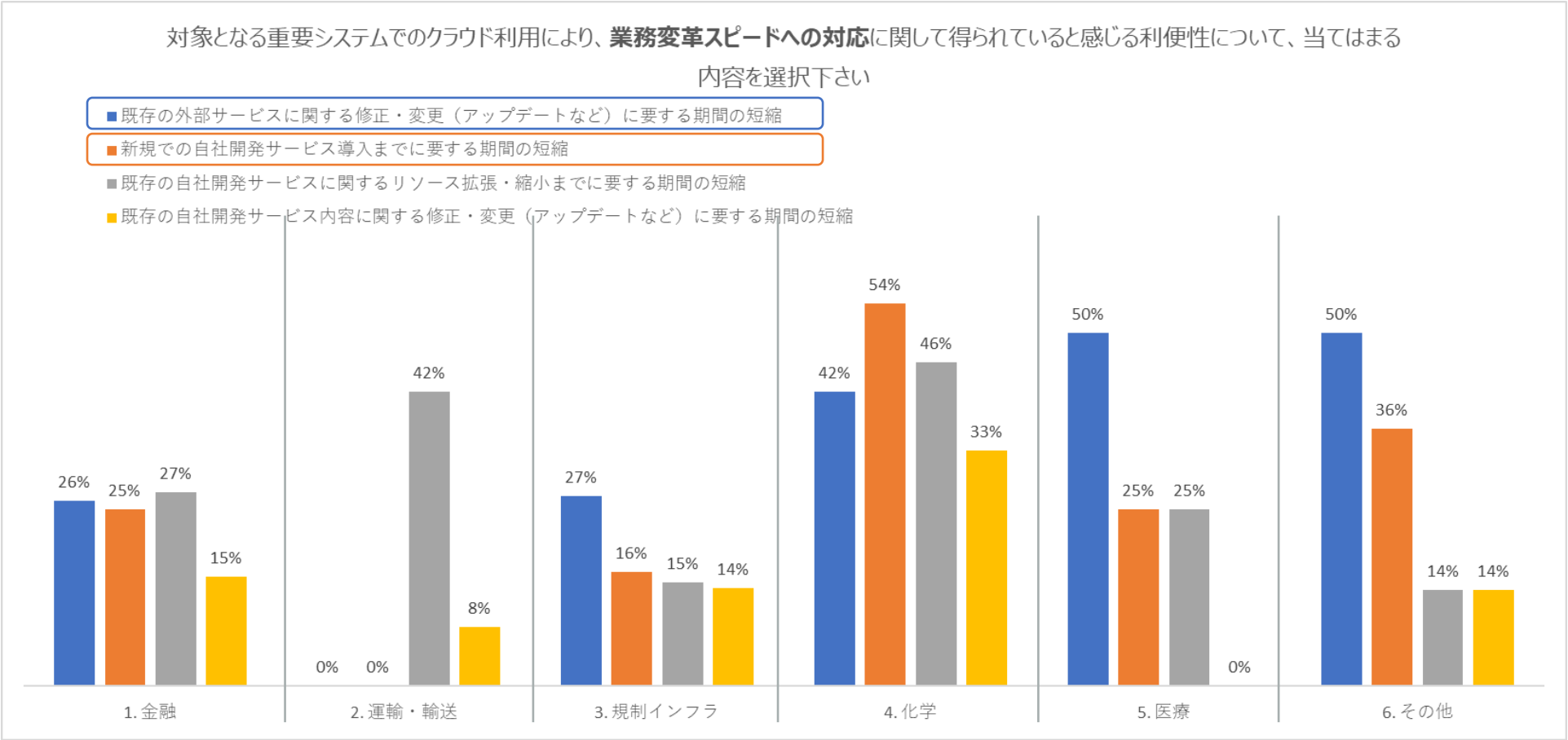
重要システム数

クレジット： 2
銀行： 12
鉄道： 4
物流： 4
ガス： 3
電力： 3
情報通信： 4
化学： 2
医療： 2
その他： 1
自動車： 1
鉄鋼： 1
熱供給： 1

アンケート結果：積極利用企業 業務変革スピード面で得られている利便性

既存外部サービスの修正・変更や、新規自社開発サービス導入のスピードの利便性を高く感じている

積極利用グループ
金融： n=32
運輸・輸送： n=3
規制インフラ： n=43
化学： n=12
医療： n=2
その他： n=22

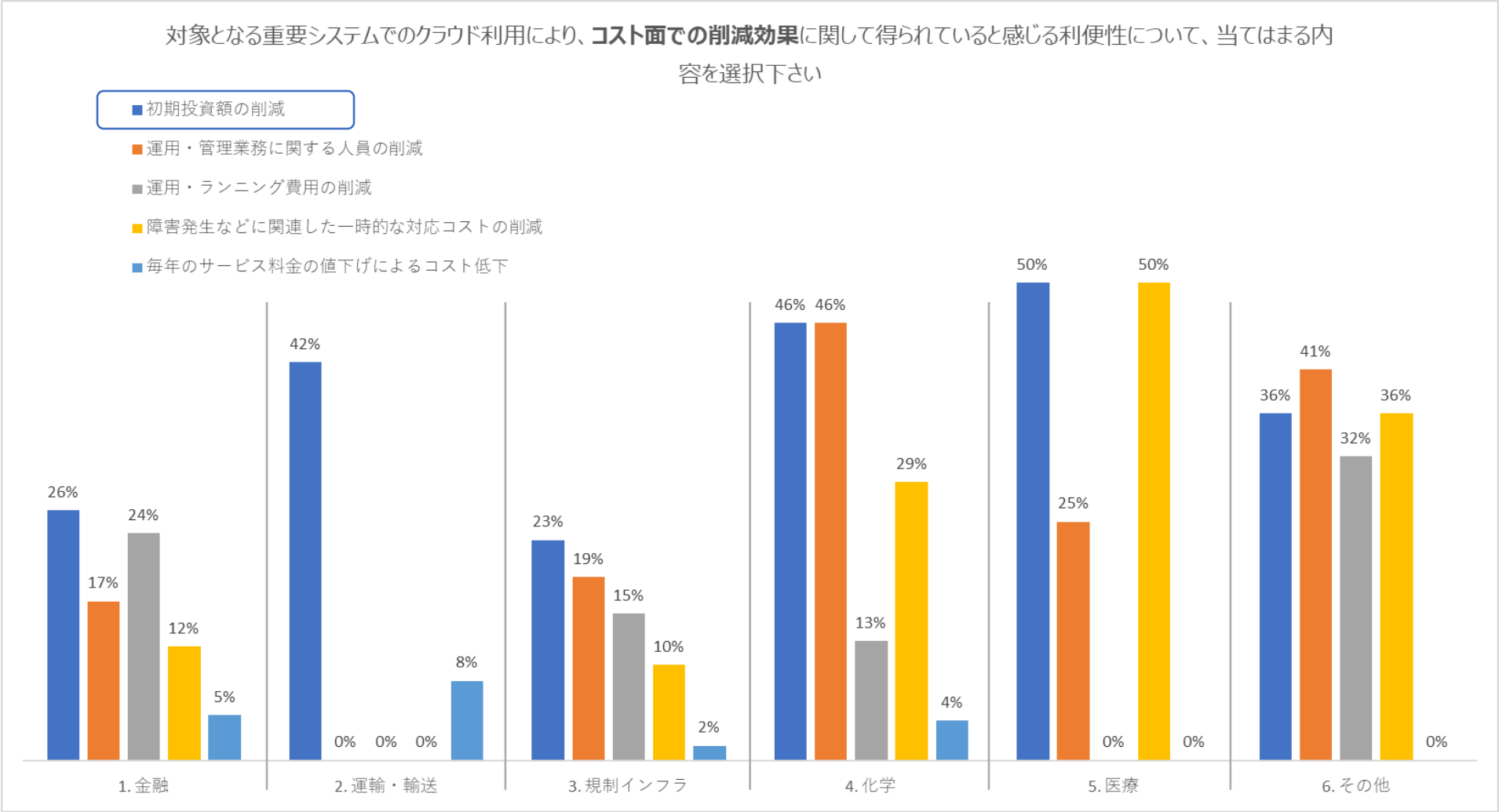


重要システム数
クレジット： 2
銀行： 12
鉄道： 4
物流： 4
ガス： 3
電力： 3
情報通信： 4
化学： 2
医療： 2
その他： 1
自動車： 1
鉄鋼： 1
熱供給： 1

※「2.運輸・輸送」および「5.医療」の積極利用グループ企業はn数が少ない為、回答結果には留意が必要

アンケート結果：積極利用企業 コスト面で得られている利便性

多くの業種で、初期投資額の削減メリットを得られている



積極利用グループ

- 金融： n=32
- 運輸・輸送： n=3
- 規制インフラ： n=43
- 化学： n=12
- 医療： n=2
- その他： n=22

重要システム数

- クレジット： 2
- 銀行： 12
- 鉄道： 4
- 物流： 4
- ガス： 3
- 電力： 3
- 情報通信： 4
- 化学： 2
- 医療： 2
- その他： 1
- 自動車： 1
- 鉄鋼： 1
- 熱供給： 1

※「2.運輸・輸送」および「5.医療」の積極利用グループ企業はn数が少ない為、回答結果には留意が必要

クラウド導入に関する懸念や課題：調査結果サマリ

セキュリティ、コスト、人材不足が懸念として挙げられた。クラウド利用が無い企業はセキュリティを懸念し、積極利用の企業はクラウドに精通した人材の確保や育成を懸念としてあげる傾向にある。また、ベンダーロックインに対する懸念も根強い

クラウドサービスの
利用拡大に向け、
どのような**懸念**
点・課題がある
か？

クラウド利用が少ない企業ほどセキュリティに強い懸念。特に利用者側の設定ミスによるセキュリティリスクを指している

- セキュリティ面の懸念がトップ。利用度合いに関わらず、多くの企業がセキュリティの懸念を強く持っているが、利用無し、消極利用、積極利用の順で高い [アンケート調査]
- 利用者側の設定ミスによるセキュリティリスクを懸念している。設定ミスには、スキル不足によるものと、人為的な誤りによるものがある
 - スキル不足による設定ミスを懸念 [A社、D社、J社]、人為的な誤りによる設定ミスを懸念 [B社、C社]
 - クラウドに載せたから安心と極端に考える顧客もいる。あまりにもクラウド事業者に頼り過ぎる顧客もいる。クラウドのセキュリティ事故はユーザーサイドでの設定ミスによることが多いということが情報発信されているものの、その誤解は無くなっていない [クラウド事業者ヒアリング]
- 利用者側の設定ミス以外では、既知の脆弱性対策の実施がクラウド事業者に依存する、クラウドと接続するために既存の閉域ネットワークに穴をあける必要がありその接続点へのセキュリティリスクを懸念している [D社、I社]
- セキュリティは、クラウドの仕組みを正しく理解している現場と漠然としか理解できていないリーダー層との違いが大きく出るところ。問題が起きるとメディアが強調して公表するので、漠然とした不安を持っているリーダーが多い。セキュリティへの理解や、運用体制が出来ているかどうかをリーダーが理解できないと利用が進まない [クラウド事業者ヒアリング]

コスト面はセキュリティに次いで懸念が高い

- コスト面はセキュリティに次いで懸念が高い項目。従量課金によるコスト制御の難しさへの懸念が全体的に高い [アンケート調査]
- 結果としてクラウドの方が高い、安くならない、という声はよくある。クラウドの特性を捉えたアーキテクチャの重要性を常に強調している [クラウド事業者ヒアリング]
- クラウドにおいてもオンプレと同じ設計思想を踏襲してしまうと、無駄なキャパシティを確保するなど、クラウドのコスト削減メリットを享受できないことがある。クラウドの特性を生かした設計や運用が行えているか、PDCAを回すことでコストの最適化を図ることが重要 [クラウド事業者ヒアリング]

クラウドを積極的に利用する企業ほど、人材を懸念としてあげている

- 社内制度・人材は、クラウドを積極的に利用する企業ほど高い懸念として挙げている [アンケート調査]
- 具体的に不足している人材としては、クラウドの特性を理解し、ビジネスやITシステムに落とし込める人材、システム開発できる人材、としている。対策として、社員の育成を進める一方で、クラウド事業者やクラウドの知見や実績のあるパートナーと連携しクラウド化を進めながら知見やノウハウを蓄積している [A社、H社、I社、J社]
- クラウド人材の育成は進んでいるが、クラウドセキュリティ人材の確保を懸念している企業もある。クラウドセキュリティ人材についての定義から検討を進めている [E社]

特定クラウド事業者に依存するリスク、ベンダーロックインによる交渉力の低下も大きな懸念

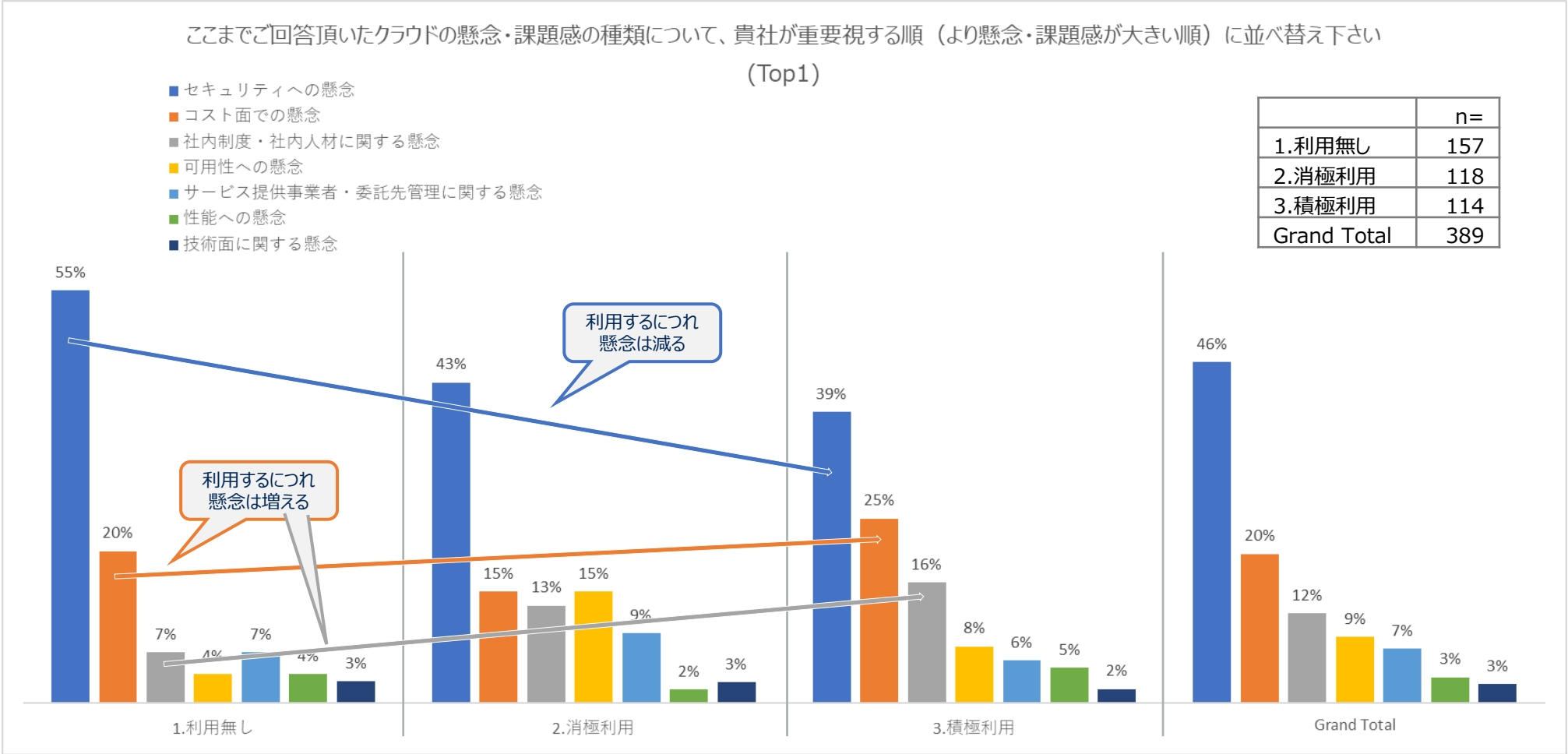
- 特定クラウド事業者のサービスへの依存度が高くなると利便性のメリットは拡大するが、他方、別のクラウドサービスへの移植性確保が難しくなる。この状況をふまえ、クラウド事業者の事業撤退リスクや価格リスクを懸念している [A社、C社、D社、E社、G社、I社]
- 利便性を高めれば高めるほど、クラウド事業者特有のサービスになってしまうので、顧客側での利便性とベンダーロックのバランスをとることが重要になる [クラウド事業者ヒアリング]

可用性を重視する企業にとっては性能は大きな懸念

- 出荷指示や配送完了通知等のトランザクションが多いため、クラウド化によって通信や処理の遅延・揺らぎがあるとエラーが起こる可能性があり、業務に支障が出ることを懸念している [B社]

アンケート結果：クラウドに対する懸念・課題感 Top1

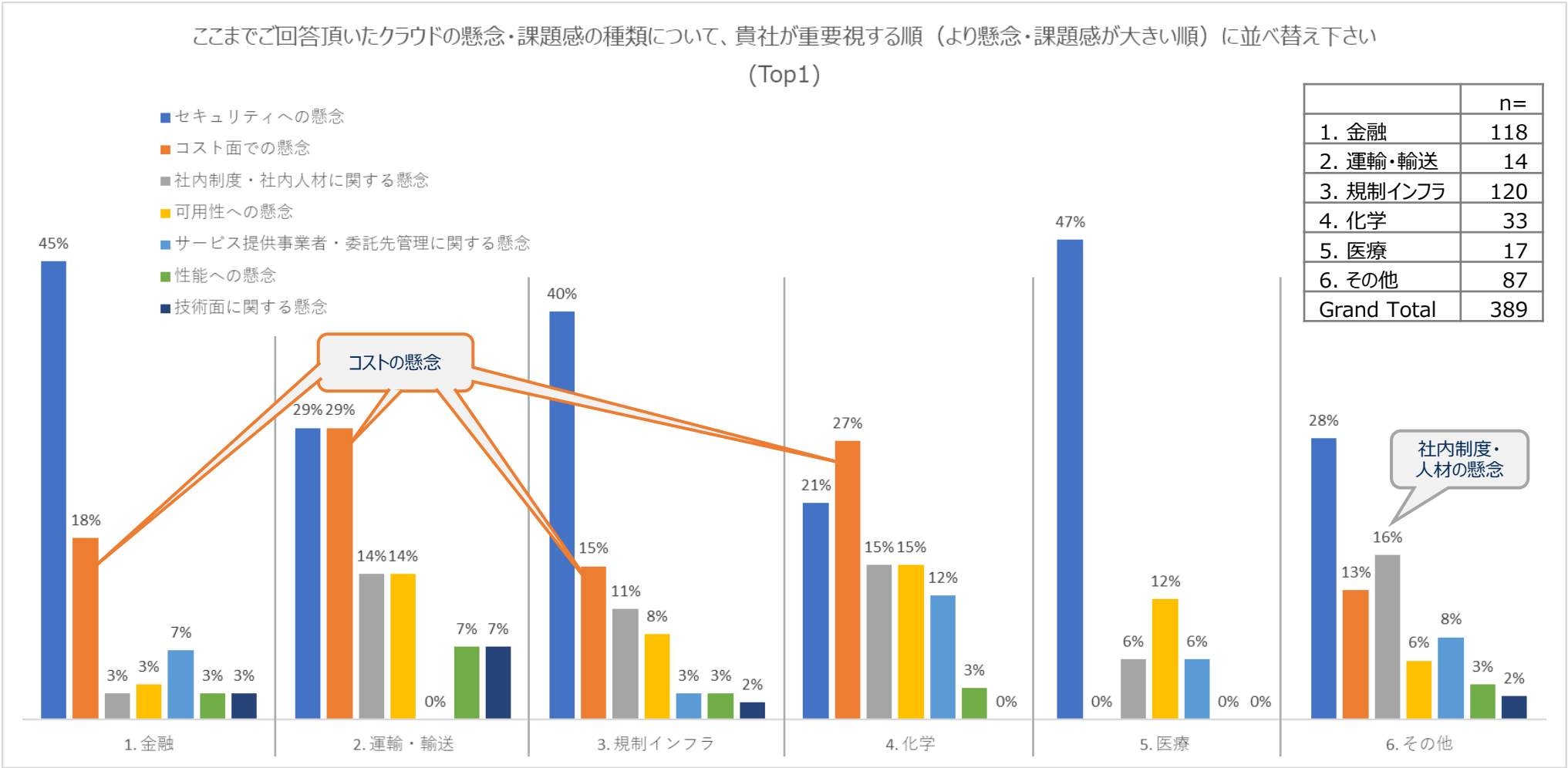
セキュリティ面の懸念が最も高く、利用の無い企業ほど懸念を強く持っている。次いでコスト面、社内制度・人材、可用性についての懸念が高く、使うほどに懸念が高まる



※利用無し＝基幹系システムにおけるクラウド利用が0%と回答した企業
※消極利用＝基幹系システムにおけるクラウド利用が25%未満と回答した企業
※積極利用＝基幹系システムにおけるクラウド利用が25%以上と回答した企業

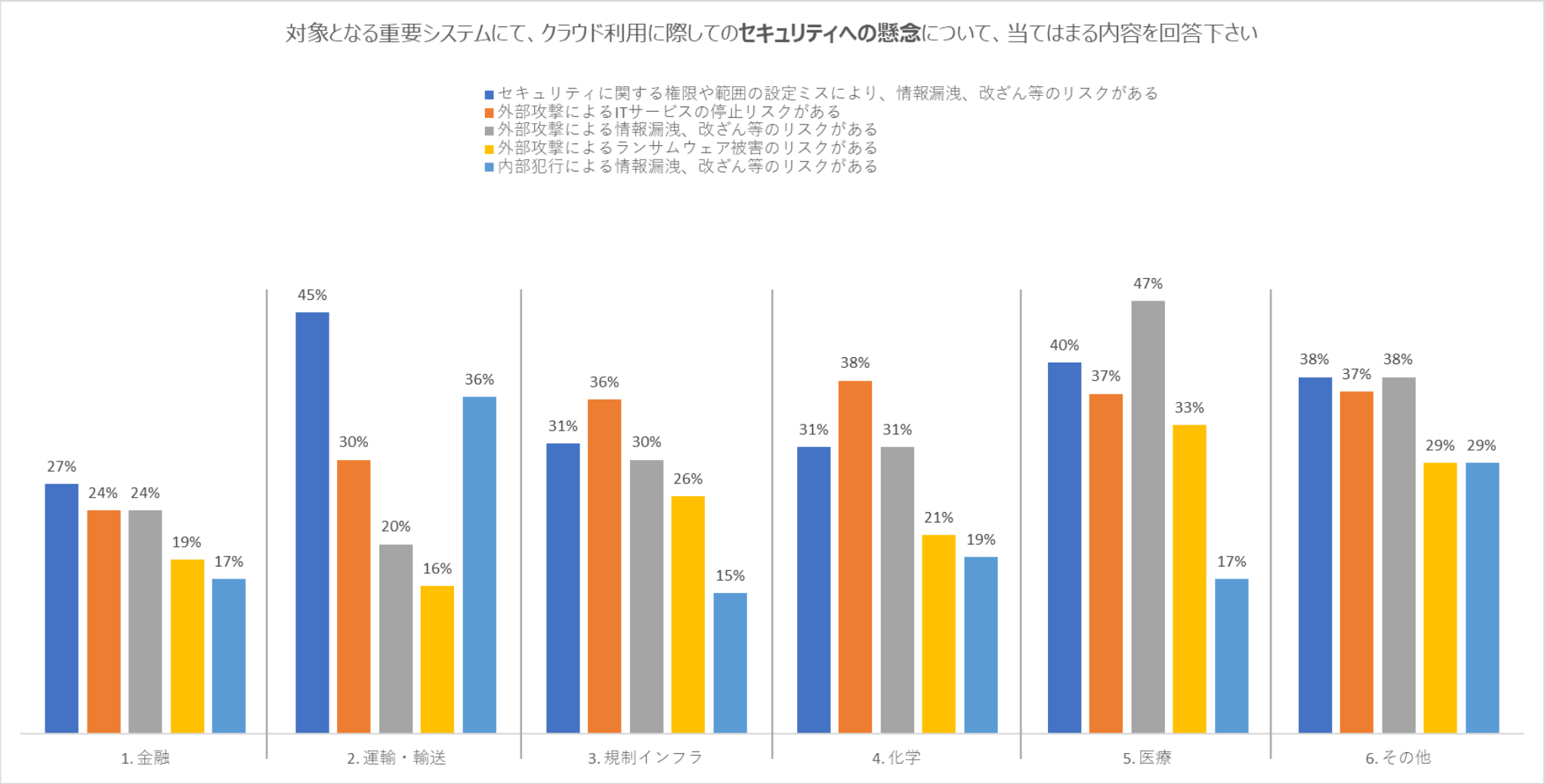
アンケート結果：クラウドに対する懸念・課題感 Top1（業種別）

セキュリティ以外では、金融・運輸・規制インフラ・化学ではコスト面、医療では可用性、その他業種で社内制度・人材への懸念が高い



アンケート結果：消極利用・利用無し企業 セキュリティ面での懸念

特に懸念が突出して強い点はなく、全てのリスクに一定以上の懸念を持っている



消極・利用無しグループ

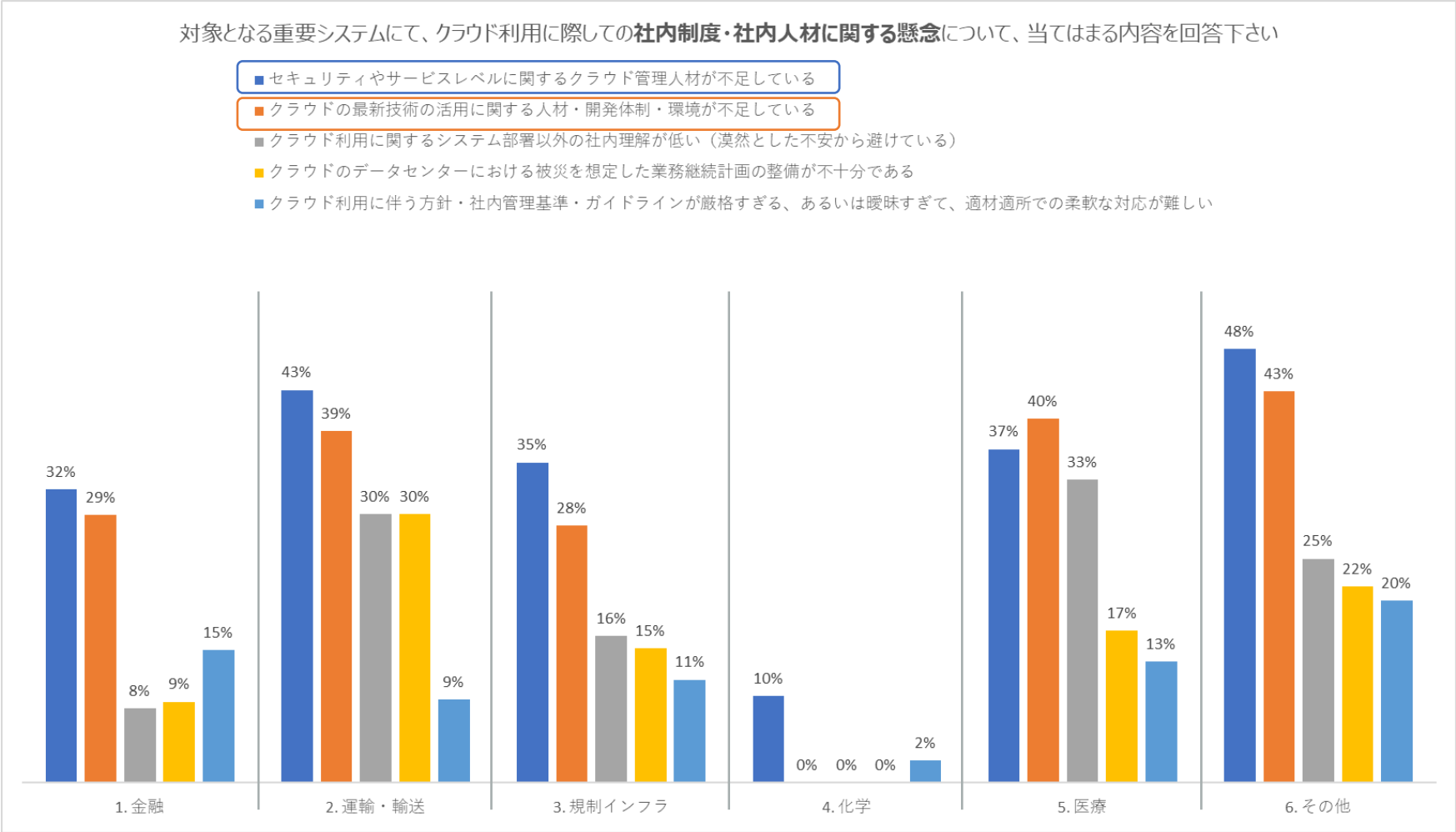
- 金融： n=86
- 運輸・輸送： n=11
- 規制インフラ： n=77
- 化学： n=21
- 医療： n=15
- その他： n=65

重要システム数

- クレジット： 2
- 銀行： 12
- 鉄道： 4
- 物流： 4
- ガス： 3
- 電力： 3
- 情報通信： 4
- 化学： 2
- 医療： 2
- その他： 1
- 自動車： 1
- 鉄鋼： 1
- 熱供給： 1

アンケート結果：消極利用・利用無し企業 社内制度・社内人材での懸念

どの業種でもクラウド管理人材の不足や、体制・環境の不足が課題となっている



消極・利用無しグループ

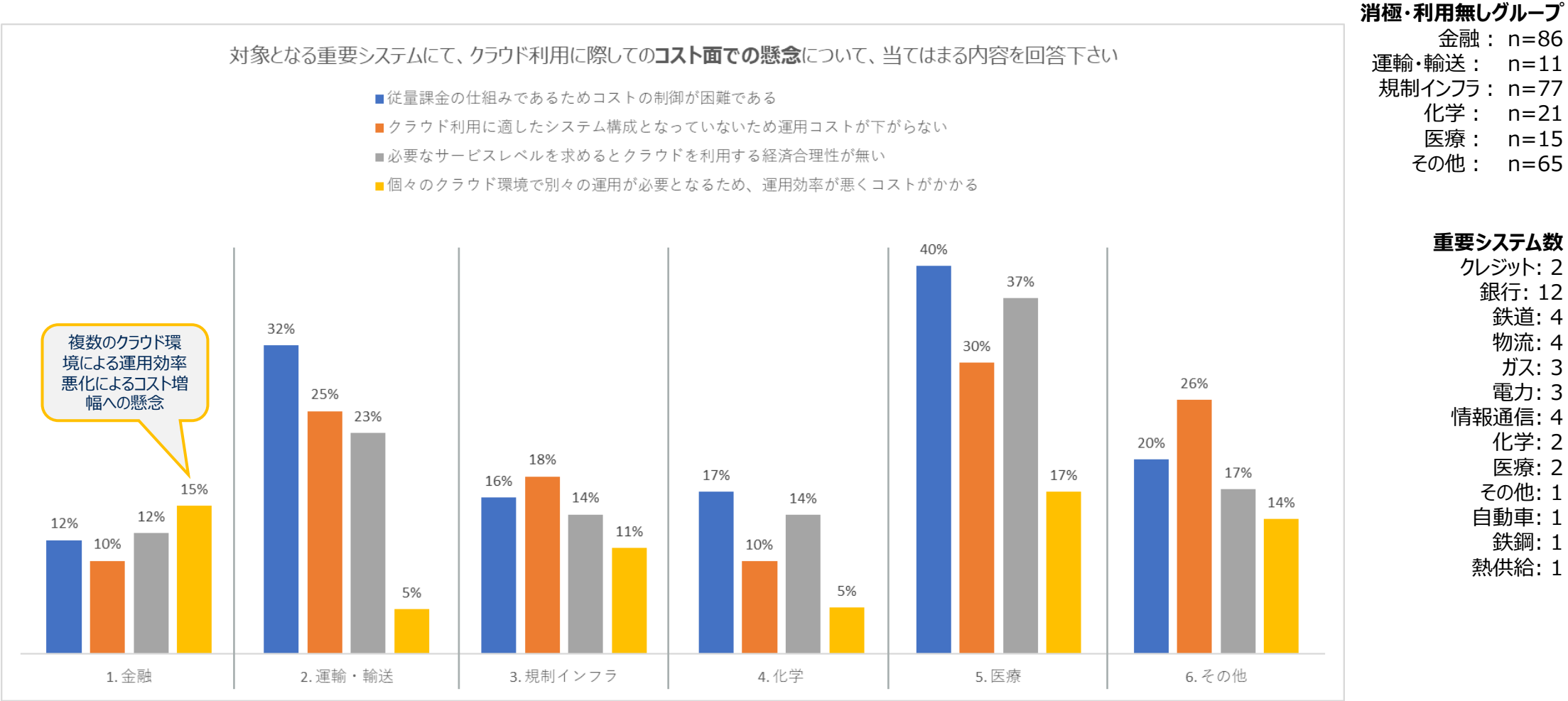
金融： n=86
運輸・輸送： n=11
規制インフラ： n=77
化学： n=21
医療： n=15
その他： n=65

重要システム数

クレジット： 2
銀行： 12
鉄道： 4
物流： 4
ガス： 3
電力： 3
情報通信： 4
化学： 2
医療： 2
その他： 1
自動車： 1
鉄鋼： 1
熱供給： 1

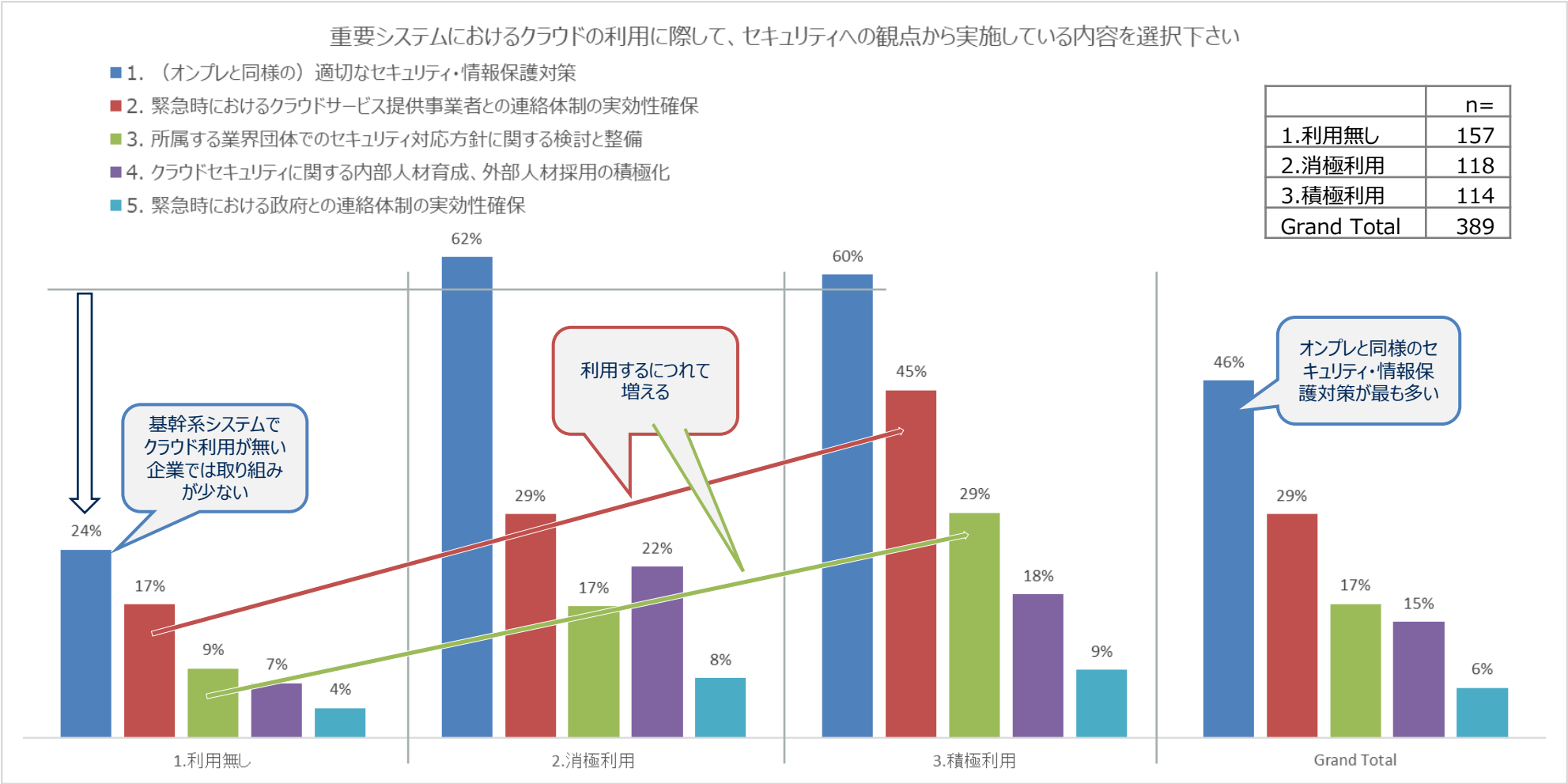
アンケート結果：消極利用・利用無し企業 コスト面での懸念

従量課金によるコスト制御の難しさへの懸念が全体的に高い中、金融では、複数のクラウド環境による運用効率悪化によるコスト増幅への懸念が高い



アンケート結果：実施施策（セキュリティの観点）

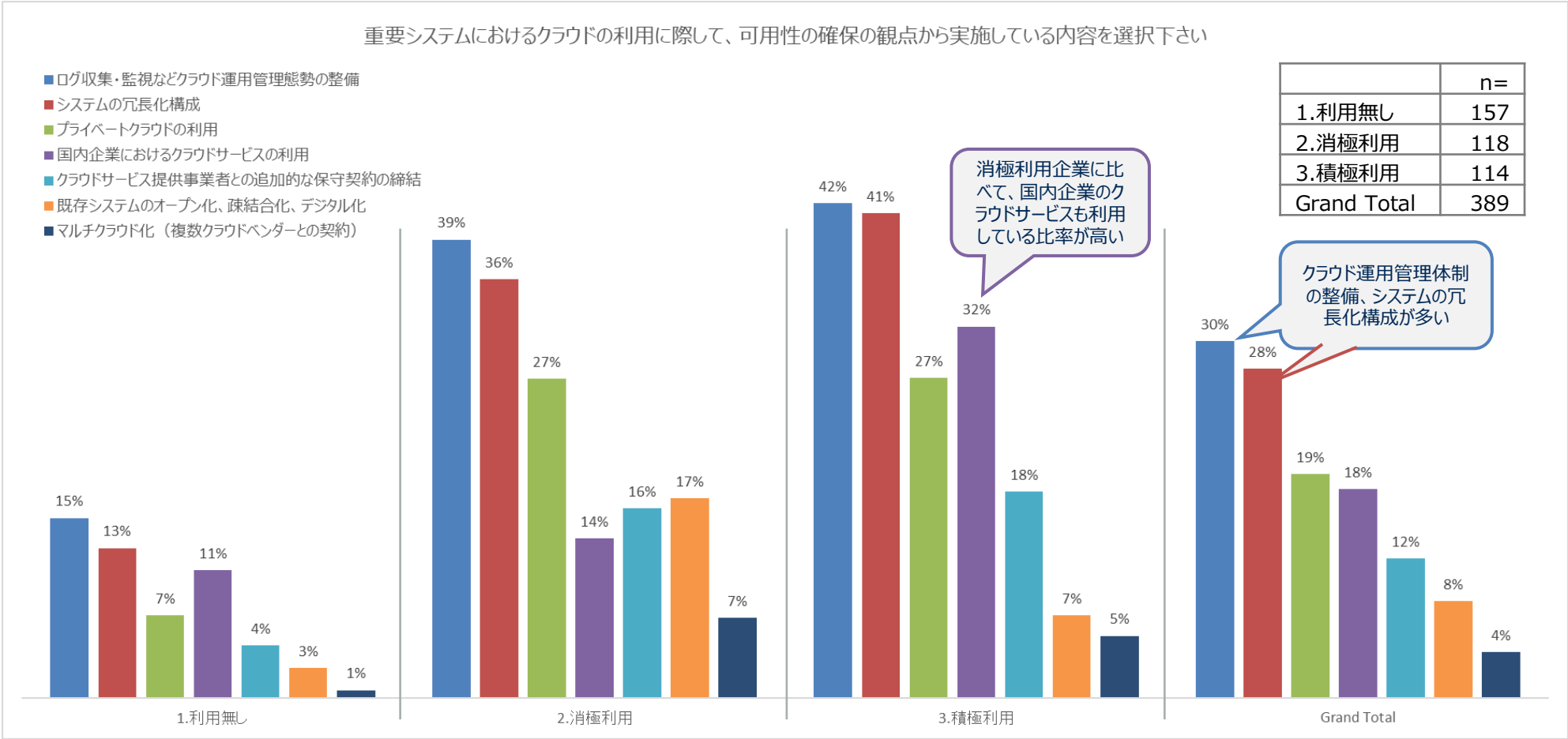
企業が自社で実施している取り組みとしては、オンプレと同様のセキュリティ・情報保護対策は最も多く、約半数が実施しているが、基幹系システムでクラウド利用が無い企業では24%と少ない。次いでクラウド事業社との連絡体制確保、業界団体での方針整備が、利用するにつれて増える



※利用無し＝基幹系システムにおけるクラウド利用が0%と回答した企業
※消極利用＝基幹系システムにおけるクラウド利用が25%未満と回答した企業
※積極利用＝基幹系システムにおけるクラウド利用が25%以上と回答した企業

アンケート結果：実施施策（可用性確保の観点）

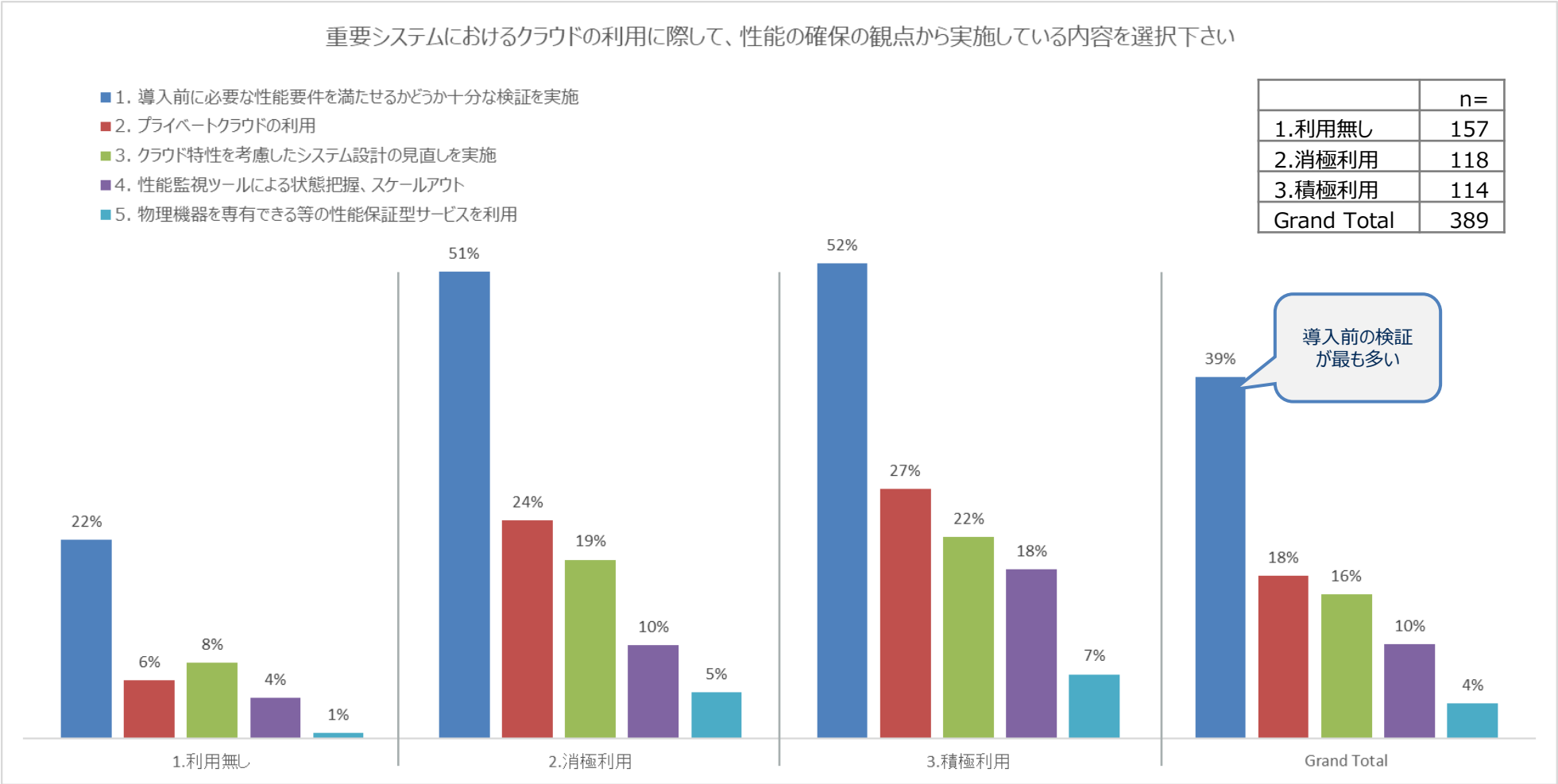
クラウド運用管理体制の整備、システムの冗長化構成が多い。積極的にクラウドを利用している企業は、消極的な企業に比べて、国内企業のクラウドサービスも利用している比率が高い



※利用無し＝基幹系システムにおけるクラウド利用が0%と回答した企業
※消極利用＝基幹系システムにおけるクラウド利用が25%未満と回答した企業
※積極利用＝基幹系システムにおけるクラウド利用が25%以上と回答した企業

アンケート結果：実施施策（性能確保の観点）

導入前の検証が最も多く、利用度によって傾向は大きく変わらない



※利用無し＝基幹系システムにおけるクラウド利用が0%と回答した企業
※消極利用＝基幹系システムにおけるクラウド利用が25%未満と回答した企業
※積極利用＝基幹系システムにおけるクラウド利用が25%以上と回答した企業

期待されるクラウド関連技術：調査結果サマリ

データバックアップのほか、シームレスなマルチクラウドを実現する技術、処理性能や低遅延を実現する技術への期待が高く、マネージドサービスやインダストリークラウドは今後普及していく見込みがある。一方でクラウドを利用していない企業は関心が低いことも分かった

懸念点・課題を解消する上で、クラウドサービス事業者やテクノロジーに期待することは？

全体的にデータバックアップへの期待が高い

- クラウドデータバックアップへの期待が最も高く、利用度によってその傾向は大きく変わらない [アンケート調査]

特定クラウド事業者への依存リスクを解決する、マルチクラウドをシームレスに利用する技術への期待が高い

- クラウド事業者の事業撤退リスクや価格リスクへの対策として異なるクラウドサービス間をシームレスに利用できる技術へ期待 [A社、E社、G社]
- 特定クラウド事業者への依存リスクへの対策以外に、プライベートと複数のパブリッククラウドを相互連携できるようにしたいため当該技術に期待する企業もある [F社]

さらなるクラウド活用を推進する上では、性能確保や低遅延を実現する技術への期待が高い

- 既存システムでメインフレームを利用している企業では、同様の処理性能をクラウドで確保する必要性をあげている
 - 現行システムでは夜間にバッチ処理している、クラウド移行後にも同様の処理能力を確保したい [D社]、今後具体的な検討を実施予定 [A社]
- 医療では低遅延の技術への期待も高い
 - リモート診断において患者の表情がクリアに見えることが重要 [H社]、取り込んだ画像を1秒程度で表示させることが重要 [I社]
- オンプレ上のデータと連携した際のレスポンスの速さを実現する技術へのニーズが今後高まる
 - クラウドはもともと全部クラウドに載せてもらうものだったが、マイグレーションに時間がかかったり、オンプレ上のデータとのレイテンシーの問題などにより、顧客のオンプレ上のデータにいかにつけていくかのニーズが高まり、そのための技術が進んできている。エッジ、分散クラウドの普及の流れは今後高まる [クラウド事業者ヒアリング]

マネージドサービスの活用は今後のクラウド普及のポイントとなる

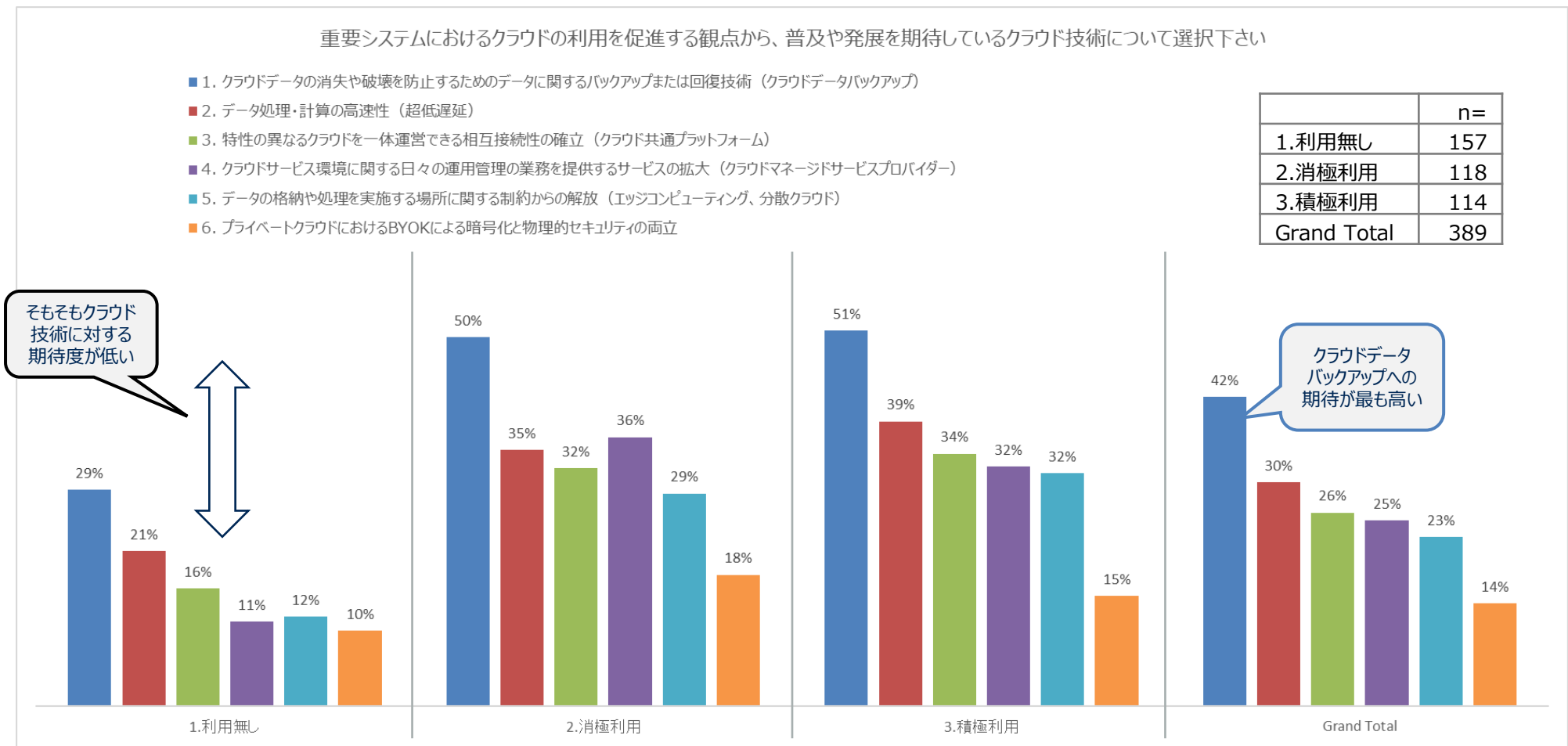
- 企業からすると、クラウド導入によって委託する範囲が拡大するが、マネージドサービスを活用できるかどうかによって負荷が変わるので、今後ポイントになると思う。グローバルでもマネージドサービス活用が進んできている [クラウド事業者ヒアリング]

インダストリー特性と捉えたサービスや機能が今後増えていく

- 事業者としてもインダストリーフォーカスを言い始めており、インダストリー特性を捉えたサービスや機能を強化している。ただし、普及はニーズ次第。専用のものはその分コストが高くなるため、要件として特別なものが必要なのかどうかによる [クラウド事業者ヒアリング]

アンケート結果：期待されるクラウド関連技術

クラウドデータバックアップへの期待が最も高く、利用度によって傾向は大きく変わらない。基幹系システムにおけるクラウド利用が無い企業は、そもそもクラウド技術に対する期待度が低い傾向がみられる



※利用無し＝基幹系システムにおけるクラウド利用が0%と回答した企業
※消極利用＝基幹系システムにおけるクラウド利用が25%未満と回答した企業
※積極利用＝基幹系システムにおけるクラウド利用が25%以上と回答した企業

クラウドに関連する制度への期待：調査結果サマリ

多くの企業が業界別の具体的なガイドラインを求めている。認定制度や情報提供義務、サービス提供義務など、クラウド事業者に関する制度への企業の期待も高い。事業者からは、特定業種に留まらず、省庁とのコミュニケーションを更に増やして欲しいという要望が挙がった

普及や発展を期待しているクラウドに関連する**制度**は？

政府に期待することは？

懸念の多いセキュリティ面に関する業種別ガイドラインが求められている

- 業種を問わず、セキュリティに関する業種別ガイドラインの普及への期待が最も高く、特に、消極利用では6割。[アンケート調査]

クラウド事業者の認定制度やクラウドへの保存可能な情報定義や対策に関する情報提供への期待は高い

- クラウド事業者の審査を個別に実施している企業では、クラウド事業者を認定する制度の活用を期待 [C社、D社、F社、G社]
- クラウド利用に際し、クラウドに保存可能な情報の定義や、クラウドに情報保存する場合の必要な対策への具体的なユースケースや関連情報の提供ニーズが多い。政府や業界のガイドラインをもとに自社でガイドラインを策定しているが、内容の適切性や十分に不安を感じている [C社、E社、H社、I社]

クラウド事業者との交渉やクラウド事業者のサービス提供義務の規定への要望も

- 海外の大手クラウド事業者との交渉は苦慮しており、業界を超えて、日本企業が意見を合わせてクラウド事業者と調整や要望を出せると良い [J社]
- クラウド事業者の事業撤退リスクへの懸念への対策として、サービス提供義務の規定を期待 [A社]

政府機関におけるクラウドの積極的活用と、企業への競争力を高める為のクラウド利用のメッセージ発信

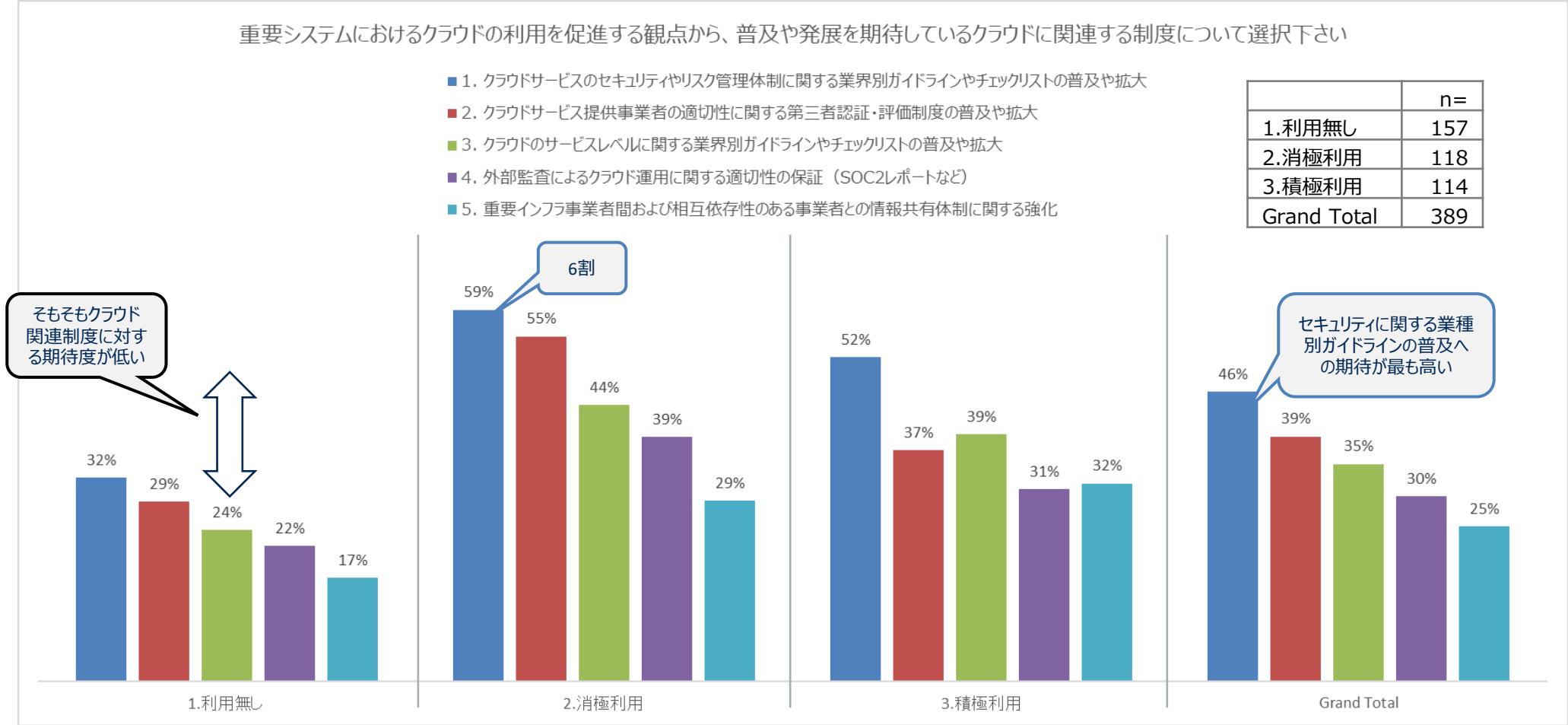
- 政府機関自身によるクラウドの積極的活用は、良いドライバになる [クラウド事業者ヒアリング]
- 「ビジネスの競争力を高める為のクラウド導入」へ舵を切っていくためのメッセージ発信を期待 [クラウド事業者ヒアリング]

各省庁とクラウド事業者とのさらなる連携強化

- より一層クラウド利用を推進していくために、各省庁はクラウド事業者とのコミュニケーションを増やして欲しい [クラウド事業者ヒアリング]

アンケート結果：クラウドに関連する制度への期待

セキュリティに関する業種別ガイドラインの普及への期待が最も高く、特に、消極利用の企業では6割。基幹系システムにおけるクラウド利用が無い企業は、そもそもクラウド関連制度に対する期待度が低い傾向がみられる



※利用無し＝基幹系システムにおけるクラウド利用が0%と回答した企業
※消極利用＝基幹系システムにおけるクラウド利用が25%未満と回答した企業
※積極利用＝基幹系システムにおけるクラウド利用が25%以上と回答した企業

5. 2021年度以降の施策展望・課題・対策

将来のクラウドサービス利用拡大にあたっての課題と対策 -サマリ

今後クラウドサービスの利用を促進していくために、技術の観点ではセキュリティ・可用性・性能・ベンダーロックインへの対策、利用者の観点では経営層や現場での推進や組織としてのクラウド利用の進め方、環境／制度の観点では政府やクラウド事業者との連携体制やクラウドサービス認定制度やガイダンスの普及が望まれる

技術の観点

- 企業がクラウド利用を進めるうえで、**セキュリティ、可用性、性能、ベンダーロックイン**に関する課題や対策を重要視している
- **【セキュリティ】クラウド事業者に預けた方が安全**と判断している一方で、**クラウド設定ミス**を懸念している。ガイドラインやツール導入等による対策を進めているが、重要情報の漏えい対策も求められる
- **【可用性】重要システムではオンプレミスと同等の要件確保**するため、高可用性のシステム構成が求められる
- **【性能】医療や工場の現場においては、高い応答速度**が求められる重要システムもあり、応答時間の低遅延化が求められる
- **【ベンダーロックイン】**クラウドの利便性拡大のため特定クラウド事業者のサービスや機能の利用度を高めると、ベンダーロックインとなりコスト等の交渉が難しくなることが懸念される。クラウドサービスを**クラウド事業者の特徴に合わせた適材適所での活用**が求められる

利用者の観点

- クラウド利用を進めるためには、最初のステップとして、経営層がビジネス変革を実現する上でのクラウド利用のメリットを理解し、**経営層によるイニシアチブによるクラウド・ファーストの推進**が求められる。また、**クラウド化しやすいシステムからクラウド利用**を開始し、クラウドに対する理解をより深め、クラウド利用を加速させる領域や慎重に進める領域を見極めることが重要となる
- クラウド利用が進むと、**現場でのクラウド人材の確保**の課題が顕著になる。クラウド利用が進んでいる企業では、クラウド事業者やパートナー企業との連携しクラウド導入を進め、その中で知識やノウハウを蓄積し、クラウド人材の定義や育成計画を策定している
- これらの取り組みはユースケースとして**クラウド利用を進める企業には参考になる**のではないかと。また、関連省庁にて情報収集し積極的に**ユースケースを情報発信**していくことがクラウド利用拡大につながるのではないかと

環境／制度の観点

- 海外の大手クラウド事業者と一企業が個別に対応していくのは限界があり、**関連省庁と、企業・業界団体やクラウド事業者が共有の課題認識のもと、一体となりクラウド利用を推進**していくことが重要ではないかと
- 関連省庁においてクラウド利用が進むことで、企業と同様の懸念や不安の共通認識をもつことができるとともに、企業のクラウド利用において必要な対策の整備が進み、企業のクラウド利用拡大に寄与するのではないかと
- 政府のクラウドサービスのセキュリティ認定制度（ISMAP）が民間企業においてクラウドサービス選定の基準になっていくことが期待され、**ISMAPを活用するための施策や、業界特性を考慮したガイダンスを普及させる施策**はクラウド利用拡大に有用ではないかと

将来のクラウドサービス利用拡大にあたっての課題と対策－技術の観点

企業がクラウド利用を進めるうえで、セキュリティ、可用性、性能、およびベンダーロックインに関する課題や対策を重要視している。対策については企業が個別に検討や検証を進めている実態をふまえると、関連省庁にてクラウド事業者のサービス開発支援や解決事例の情報発信を行うことも有用ではないか

クラウドサービス利用拡大に向けた対策（技術の観点）

【セキュリティ】利用者のクラウド設定ミスに起因するセキュリティリスクへの対策

- 業種問わず、セキュリティ面の懸念払拭は全体のクラウド利用が広がるための絶対条件である
- クラウド利用が進んでいない企業ではクラウドの責任共有モデルやセキュリティリスクへの理解不足による漠然とした懸念があると考えられる。クラウド利用が進んでいる企業ではクラウド事業者の高度なセキュリティ対策を理解し自社での対策と比較した上でクラウドを利用した方が安全と判断しているが、オンプレミスよりも厳密な設定が必要になるクラウドセキュリティに対する、利用者の理解不足によるクラウド設定ミスのリスクを懸念している
- クラウド設定ミスに対して、ガイドライン作成や設定ミスを検出するソリューション導入の対策が進みつつあるが、機密情報の漏えいに備えたデータの保管や暗号化も求められる

【可用性】オンプレミスシステムと同等の高可用性の実現

- 無停止が要求される重要システムではオンプレミスと同レベルの可用性確保が要件としている。クラウドで可用性要件を満たせない場合は重要システムはクラウド利用の対象外もしくは優先度を下げている実態がある
- クラウド事業者による重要システムの業界特有要件（可用性等）を満たす専用クラウドサービスの提供や、クラウド事業者の大規模障害発生時に可用性確保の仕組みが求められる

【性能】低遅延な環境の提供

- 医療や工場の現場において、安定的な低遅延の環境が求められる重要システムがある
- 回線帯域増に伴うコスト増を抑え、応答時間の低遅延化が求められる

【ベンダーロックイン】クラウド事業者の特徴に合わせた適材適所での活用

- クラウドの利便性をより拡大させるため、特定のクラウド事業者のサービスに依存した業務設計やマネージドサービスの利用をすすめると、他のクラウド事業者への移行が難しくなりベンダーロックインとなるリスクがある。クラウド事業者はオープンAPIを介したデータ利用などベンダーロックインを発生させないようにしているケースもあるが、固有のサービス機能を利用する場合はベンダーロックインとなってしまう。
 - 結果として、クラウド事業者が利用者よりも優位な関係となり、クラウド利用が進んでいる企業では、クラウド事業者とのコストや保守等に関する調整の難易度が上がることや、クラウド事業者の事業撤退リスクを懸念している
- 68 ■ 利用者はクラウド事業者の特徴に合わせて適材適所でクラウドサービスを選択し利用する（マルチクラウド化）ことで、ベンダーロックインのリスクを最小限にすることが求められる

将来のクラウドサービス利用拡大にあたっての課題と対策－利用者の観点

クラウド利用が進んでいる企業では、経営層のイニシアチブによるクラウド・ファーストの推進、クラウド化しやすいシステムからのクラウド利用の取組を進める、および現場におけるクラウド人材の確保と育成、ユースケースとして他企業は参考になると思料。関連省庁にて情報収集し積極的に情報発信していくことがクラウド利用拡大につながるのではないかと

クラウドサービス利用拡大に向けた対策（利用者の観点）

経営層のイニシアチブによるクラウド・ファーストの推進

- クラウド・ファーストを掲げ、経営層、とりわけビジネス部門の責任者がビジネス変革を実現する上でのクラウドの必要性を理解し、クラウド利用を進めている企業では、クラウドをどのように活用するのかの視点でガイドラインやルールを整備され、クラウド利用が進んでいる
- 他方、クラウド・ファーストを掲げているものの、クラウドを選択肢の一つとして捉えている企業では、安全性を重視する保守的なガイドラインやルールが策定され、現場においてもオンプレミスの考え方が踏襲され、クラウド利用が進みにくい実態がある
- クラウドを利用することで事業環境の変化に柔軟に対応できることを経営層が理解し、自ら推進役となって取り組むことが重要である

クラウド化しやすいシステムからクラウド利用

- クラウド利用が進んでいる企業では、情報系システムや戦略系システム、新規ビジネスのシステムなど、クラウド化しやすいシステムからクラウド利用を開始し、他システムでのクラウド利用を拡大している
- クラウドを実際に利用することでその特性を理解し、重要システムにおいて、移行や可用性等の課題やリスクを見極めた上でクラウド利用を検討していくことが重要である

現場におけるクラウド人材の確保と育成

- クラウドを導入したことでクラウド人材不足の課題が顕在化している
- クラウドの特性を理解し、ビジネスやITシステムに落とし込みクラウド利用の必要性を経営層へ説明できる人材、システム開発できる人材、クラウドセキュリティについて包括的な視点で対策を検討できる人材の確保と育成が求められる
- 一部の企業では、クラウド事業者やクラウドの知識や経験のあるパートナー企業と連携してクラウド利用を進めながら、人材の育成や知見／ノウハウを蓄積するなど、クラウド人材の育成を計画的に進めている

将来のクラウドサービス利用拡大にあたっての課題と対策－環境／制度の観点

関連省庁と、企業・業界団体やクラウド事業者が共有の課題認識のもと、一体となりクラウド利用を推進していくことが重要ではないか。また、ISMAPの企業での活用促進や業界特性を考慮したガイダンスを普及させる施策もクラウド利用拡大には有用ではないか

クラウドサービス利用拡大に向けた対策（環境／制度の観点）

関連省庁、企業・業界団体、クラウド事業者が一体となったクラウド利用の推進

- 企業は、大手クラウド事業者が海外企業であることや、国内事業者のサービス提供の安定性・継続性へ不安を抱えている。
- 海外の大手クラウド事業者と一企業が個別に対応していくのは限界があり、関係省庁と、企業・業界団体やクラウド事業者との意見交換をより活発化させ、クラウド利用拡大に向けた課題認識や必要な情報提供などを一体的に進めていくことが重要である

関連省庁におけるクラウド利用の加速

- 関連省庁においてクラウド利用が進むことで、企業と同様の懸念や不安の共通認識をもつことができるとともに、企業のクラウド利用において必要な対策の整備が進み、企業のクラウド利用拡大に寄与するのではないか

政府のクラウドサービス認定制度や、業界別ガイダンスやユースケースの普及

- クラウド利用が進んでいる企業であっても、クラウド事業者の審査や自社で策定したクラウド利用のガイドラインやルールの十分性を懸念している。クラウド事業者の認定制度や、重要システムに高可用性が求められる、コスト削減を最優先するなど業界特性を考慮したクラウド利用に関するガイダンスやユースケースの提供により、企業がより安心、納得してクラウドを利用できる環境整備が重要となる
- クラウド事業者の認定制度については、政府によるクラウドサービスのセキュリティ認定制度（ISMAP）を民間企業や業界でクラウドサービスを選定する際の新しい基準となることが期待されており、ISMAPの活用を民間企業へ普及させていく施策が望まれる。また、ISMAPの認定クラウドサービス数は少なく、企業や業界で活用するためには認定クラウドサービスの数を増やしていくことも重要で、認定取得プロセスの自動化や簡素化も望まれる

今後必要とされるクラウドサービスの要素およびその実現に必要な技術課題

クラウドサービス利用拡大に向けた技術要件に対して対応方法はあるものの、クラウド事業者から提供されているサービスについて、機能が限定的である、独自仕様で個別対応が必要などの課題がある。普及に向けて、今後の研究開発や基準の策定等、社会実装支援に繋げていく必要がある

	クラウドサービス利用拡大に向けた技術要件	対応方法	今後必要とされる技術課題
セキュリティ	クラウド設定ミスの防止	クラウドの状態管理ツールを導入し、設定ミスや管理不備の検出や修復を継続的に行う	クラウドの状態管理ツールの大半はPaaSやIaaSに対応したものであり、一部はSaaS対応しているが、外部からの状態管理の可否がSaaSに依存し限定的となっている。企業が利用するSaaSへの対応、SaaSでの不正利用や情報漏えいにつながる設定を監視できることが必要となる
	機密情報の漏えいに備えたデータの保管や暗号化	- 機密性の高い情報はオンプレミスやプライベートで管理し、機密性の低い情報はパブリッククラウドで管理するハイブリッドクラウドを導入する - パブリッククラウド上で利用者以外はデータ複合できない暗号化技術を利用する	パブリッククラウド上で利用者以外はデータ複合できない技術（コンフィデンシャルコンピューティング等）について大手クラウド事業者では当該技術を活用したサービス提供は始まっているが、独自仕様でアプリ側でも対応が必要となるため、オープン化が望まれる
可用性	クラウド事業者による業界特有要件（可用性等）を満たす専用クラウドサービスの提供	業界で利用されるアプリ機能をパッケージした業界専用クラウドサービスはクラウド事業者から提供されているが、可用性などの非機能要件を満たす業界専用クラウドサービスは国内では未提供である	クラウド事業者の業界専用クラウドのサービス設計において、可用性の非機能要件に対し、業界で共通化できるのか、個別ニーズにどこまで対応するのか課題がある
	クラウド事業者内の大規模障害発生時にも可用性を確保をする仕組み	システムをコンテナ化し、オーケストレーションツールでコンテナ管理を実施し、障害発生時に実行環境をプライベートクラウドや他のクラウド事業者のサービスに自動的に切り替える	- 重要システムをコンテナ化できるのか課題がある - コンテナのオーケストレーションツールについて、複数のクラウド事業者のサービス上で動作させることが必要となる。また、障害検知や切り替え時間など重要システムの可用性要件を満たすことが必要となる
性能	応答時間の低遅延化	クラウド事業者が利用者の利用拠点に物理的に近い場所でパブリッククラウドのサービス（分散クラウド）を提供する	関連サービスはクラウド事業者から提供し始めた状況であり、パブリッククラウドの機能がどこまで利用できるのか、ネットワーク接続に関わる設計やコスト負担が課題である
ベンダーロックイン	クラウド事業者の特徴に合わせた適材適所での活用	- マルチクラウドの管理作業を軽減するため、マルチクラウド管理ツールの導入や管理サービスを利用し管理作業を簡素化、効率化する - コンテナ技術を活用しシステムを構築し、他のクラウド事業者のサービスへの移行を容易にする	- 管理ツールのサポートはクラウド事業者によって機能に差異があり、利用する管理機能が特定のクラウド事業者でサポートされていないケースもある - 重要システムを含めたすべてのシステムをコンテナ化できるのか課題がある

ガートナー ジャパン株式会社

ガートナー コンサルティング

〒105-6205

東京都港区愛宕2-5-1 愛宕グリーンヒルズMORIタワー5階

Tel. 03-6430-1870 Japan.Consulting@gartner.com