JUASグローバルフォーラム

2021年度分科会活動報告

- 1班　システムの標準化（グループの共通化領域、推進方法）およびデータ活用
- 2班　ベンダーマネジメント・コミュニケーションツール
- 3班　働き方の変化（含むセキュリティ）

- **1班　システムの標準化およびデータ活用**

- 2班　ベンダーマネジメント
  ・コミュニケーションツール

- 3班　働き方の変化（含むセキュリティ）

システムの標準化（グループの共通化領域、推進方法）およびデータ活用

1班メンバー

名前 （敬称略、五十音順）	所属
大宅 貴寛	FUJIFILM Business Innovation Asia Pacific
金　孝京	SUNTORY Beverage & Food Asia Pte Ltd
東前 卓也	Ricoh Asia Pacific Operations Limited
松本 陽一	Obayashi Corporation
宮川 貴薫	ITOCHU Singapore Pte Ltd

アンケート実施内容

下記分類を定義し、
主にグローバル、リージョナル、個社、不明・未導入の回答形式を実施

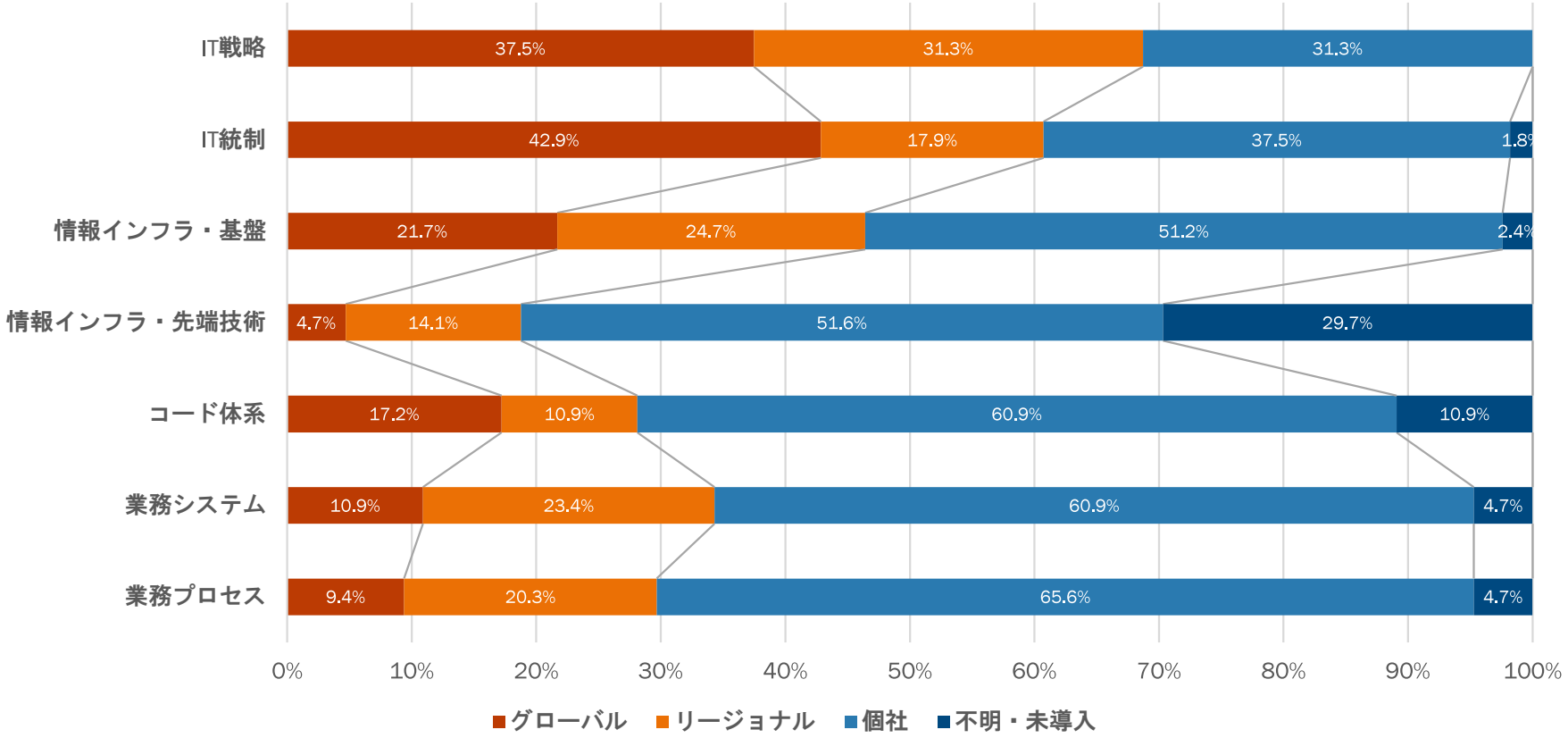
（回答数　16）

分類	アンケート詳細
IT戦略	IT戦略の企画立案レベル
IT統制	セキュリティ（訓練・教育、組織（GSOC/CSIRT））、BCP/DR、共通購買・配賦ルール、IT予算、プロジェクト実施承認・決裁
情報インフラ基盤	コミュニケーション基盤、ID管理、機器管理、データセンター、ネットワークなど
先端技術の活用	AI、IoT、RPA、ブロックチェーンの活用
コード体系	人事、購買、会計、営業システムコード
業務システム	人事、購買、会計、営業システムのアプリケーション
業務プロセス	人事、購買、会計、営業システムの業務プロセス

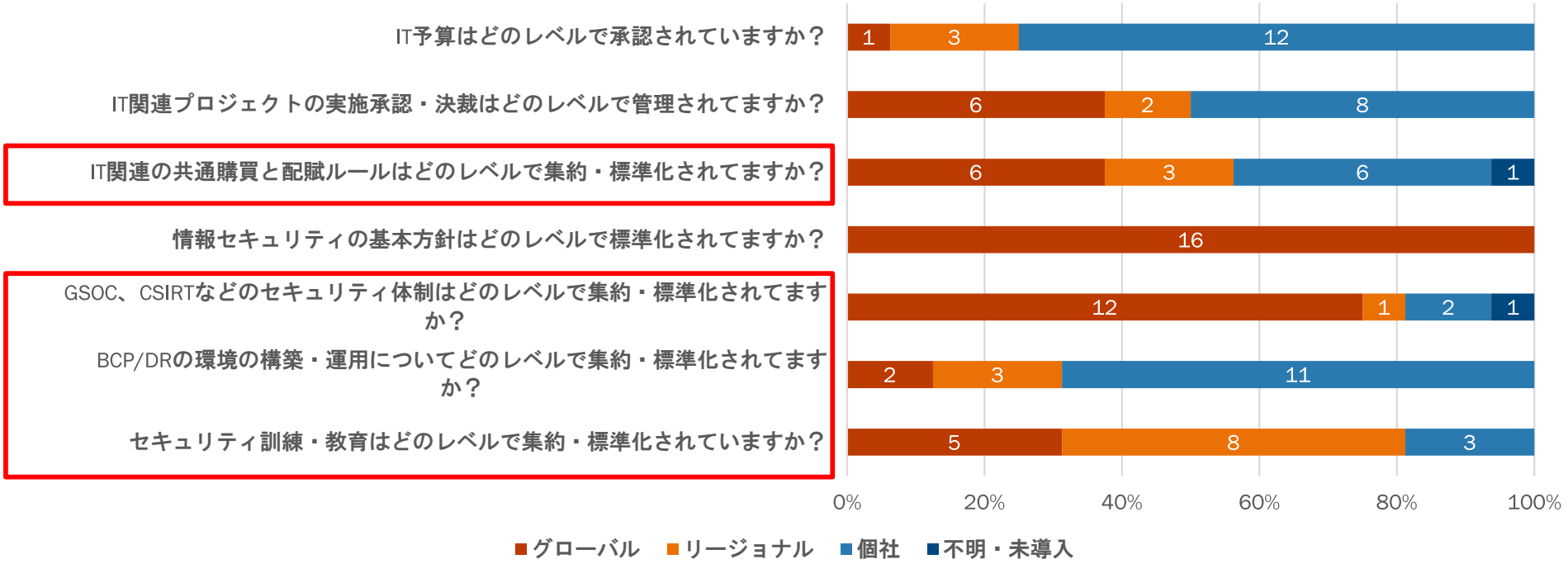
アンケート全体傾向

グローバル・リージョンでの標準化傾向

IT戦略・統制	：約半数
情報インフラ、業務システム、業務プロセス、コード体系	：約３割
先端技術の活用	：２割



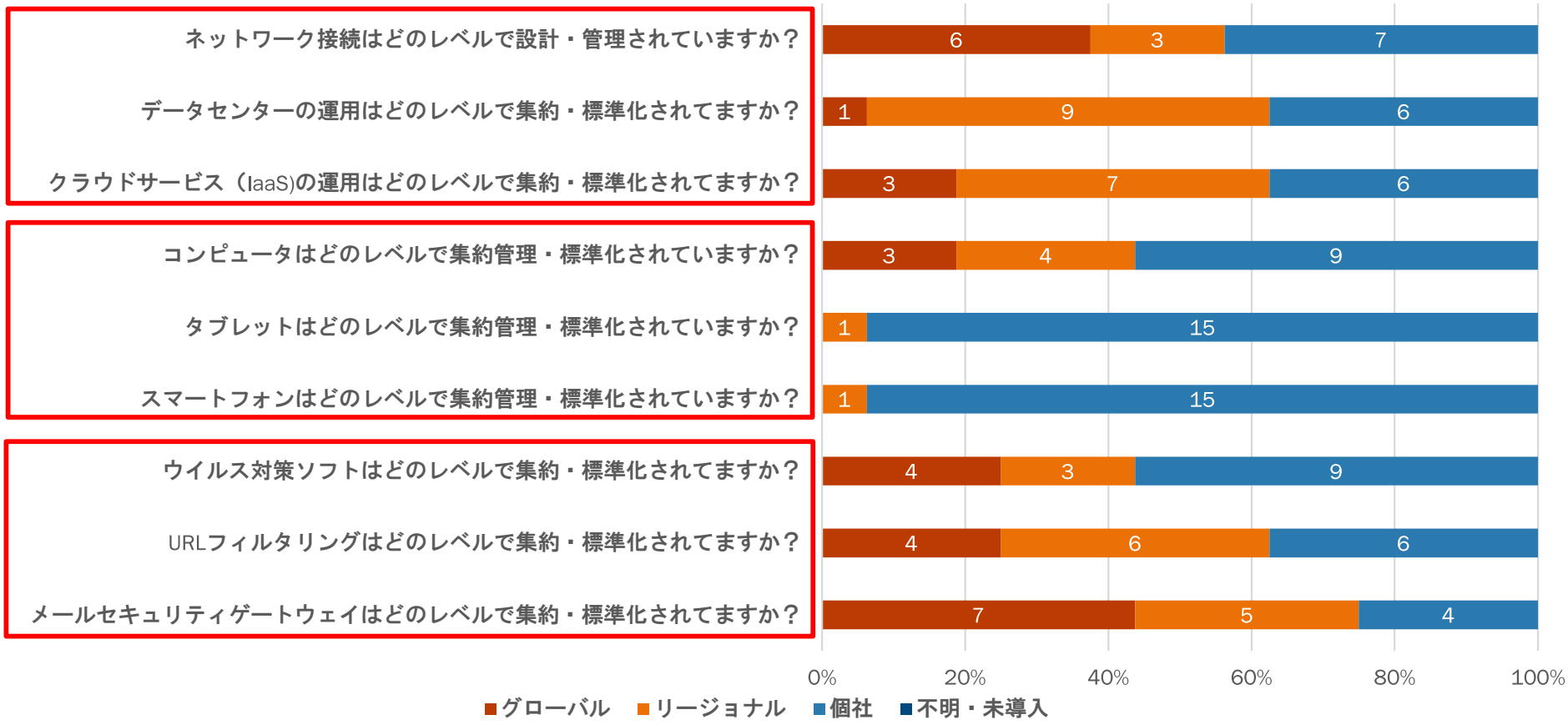
IT統制



コメント

- **<u>プロジェクト管理がEXCELのためタイムリーに管理ができない。</u>**
- IT人財育成にiCDのフレームを活用したが、日本語ベースのため適しなかった。良いフレームワーク、ソリューションがあれば紹介希望。
- **<u>情報セキュリティにおいて各社が個別で予算化・導入を行うため対策にバラつき</u>**が発生
- 標準化のレベルを設定するのが難しいし、価値観が人によって異なる点がある。Policyレベルは標準化しやすいが、プロシージャレベルは使うツールにもよるので、標準化しにくい等。

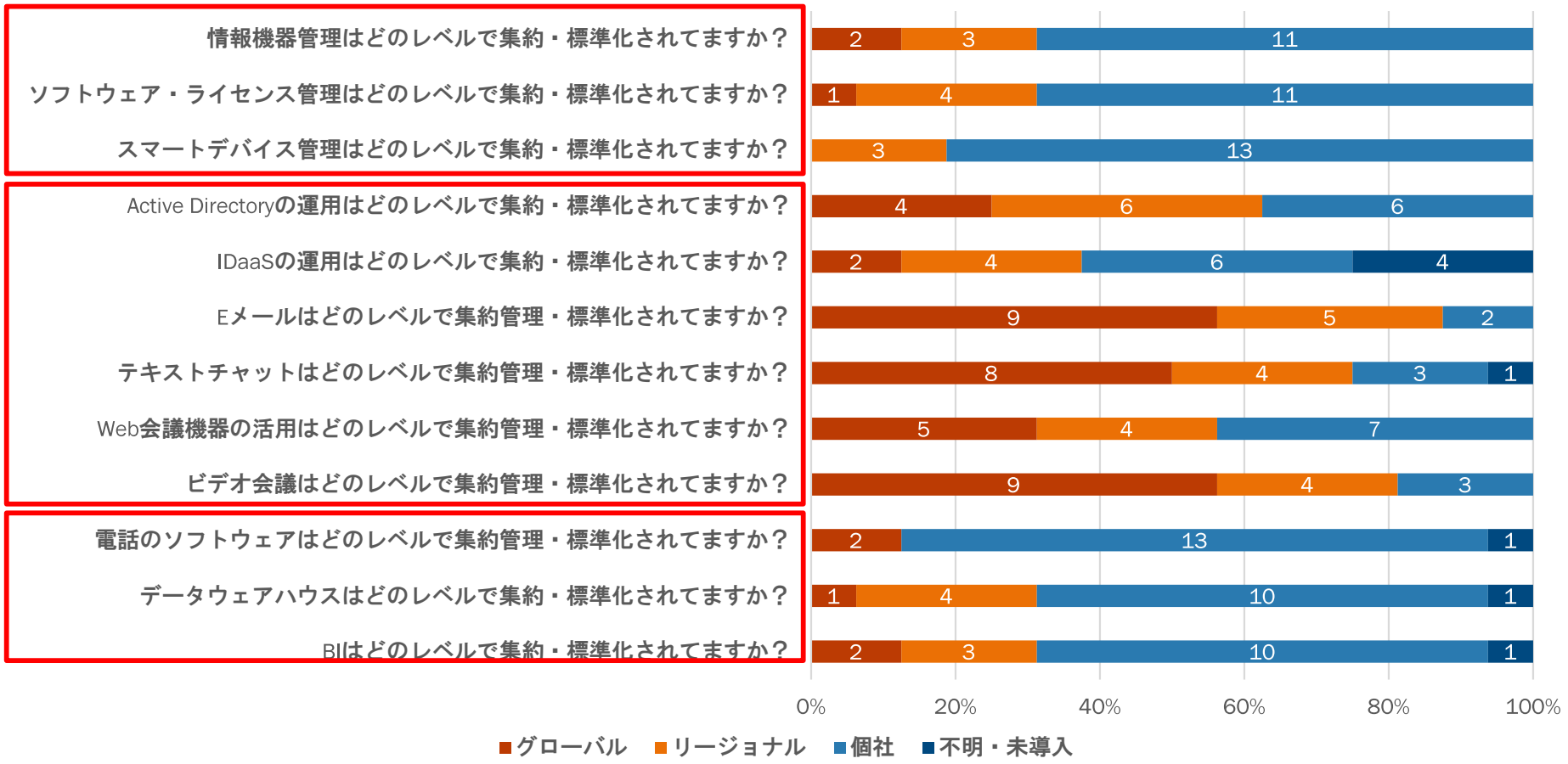
情報インフラ・基盤（１）



コメント

- **<u>国をまたいだソフトウェアライセンス管理</u>**（最低契約数に満たない各拠点の契約希望数に対し、リージョナルHQで一括管理するのか）をどこまで踏み込んで標準化するのかが課題点。グローバル標準している会社がある場合、リージョン標準と比較して、そのメリットデメリットを共有して頂けると有難い

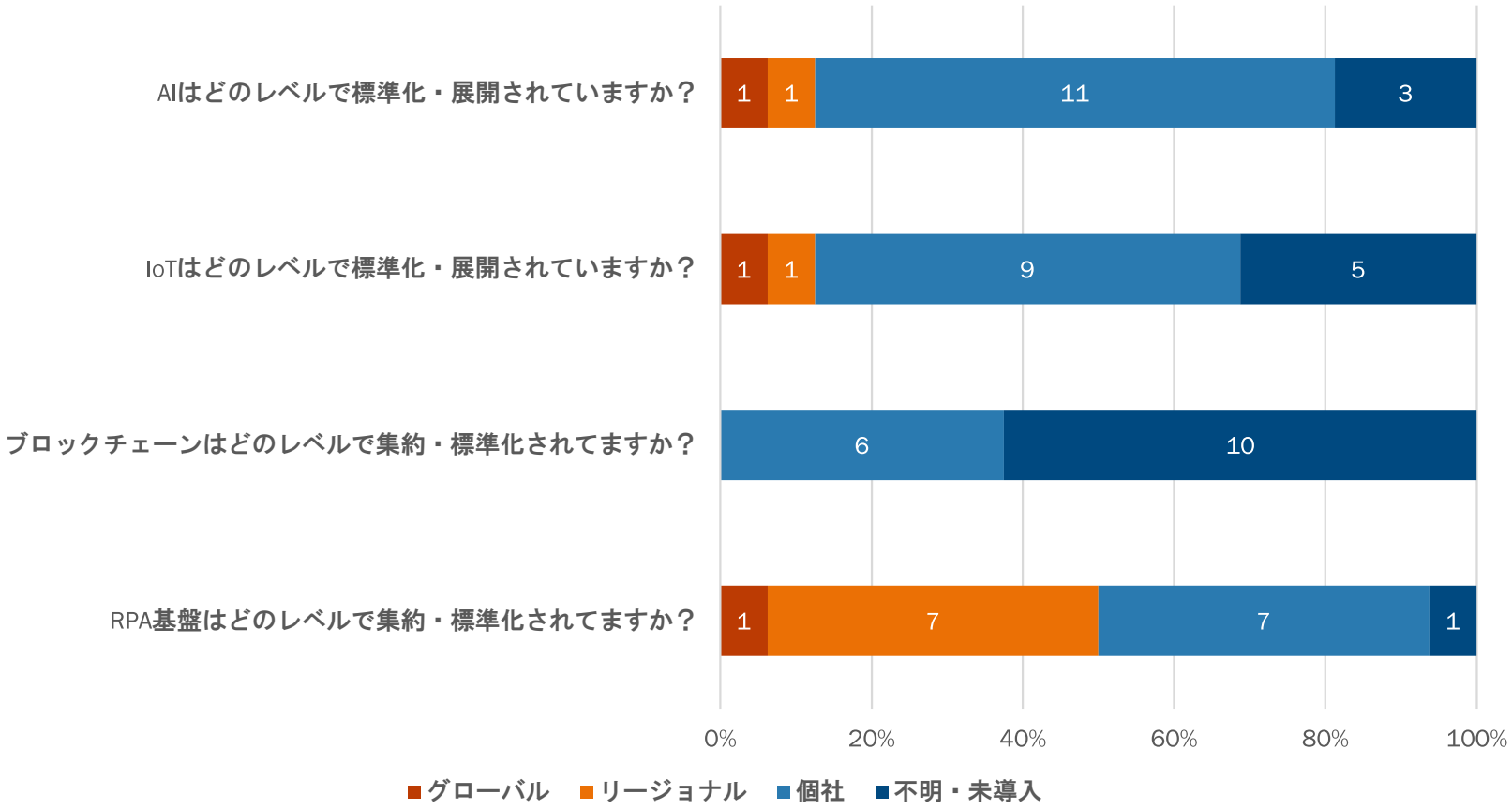
情報インフラ・基盤（２）



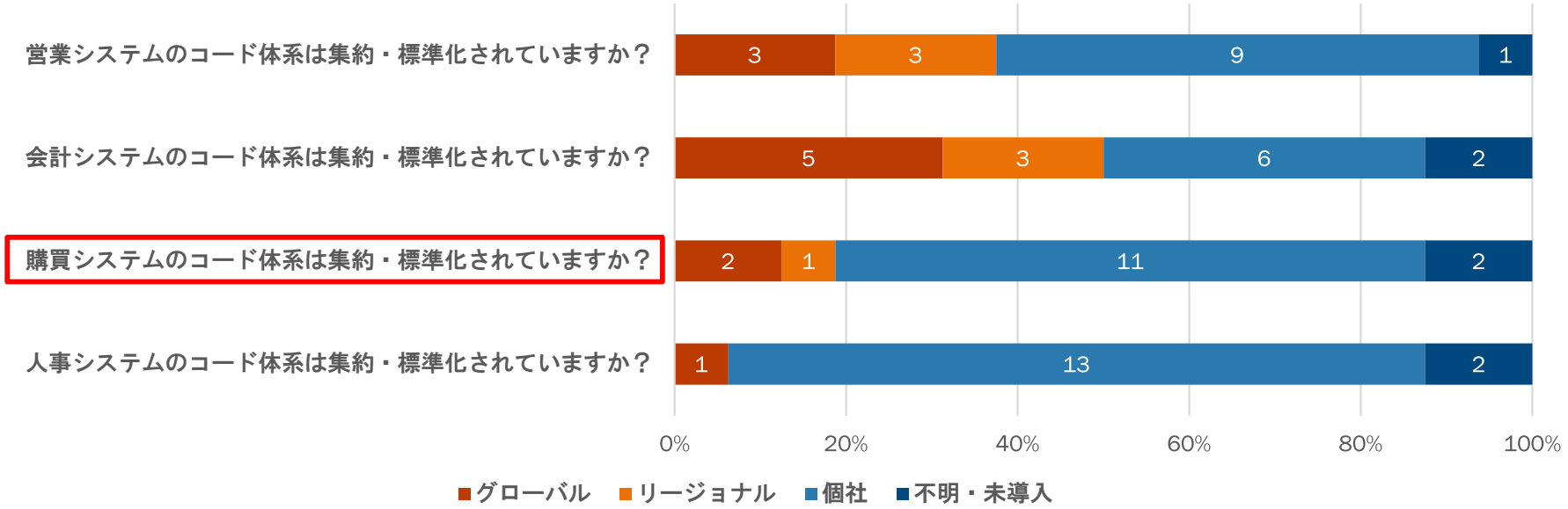
コメント

- **<u>リージョンで標準化すると個社でのコストよりも高くなる場合がある</u>こと。国毎に安い機器やサービスが違ったり、バーゲンがある。**

先端技術活用


AIはどのレベルで標準化・展開されていますか？
1
1
11
3
IoTはどのレベルで標準化・展開されていますか？
1
1
9
5
ブロックチェーンはどのレベルで集約・標準化されてますか？
6
10
RPA基盤はどのレベルで集約・標準化されてますか？
1
7
7
1
0%
20%
40%
60%
80%
100%
グローバル
リージョナル
個社
不明・未導入

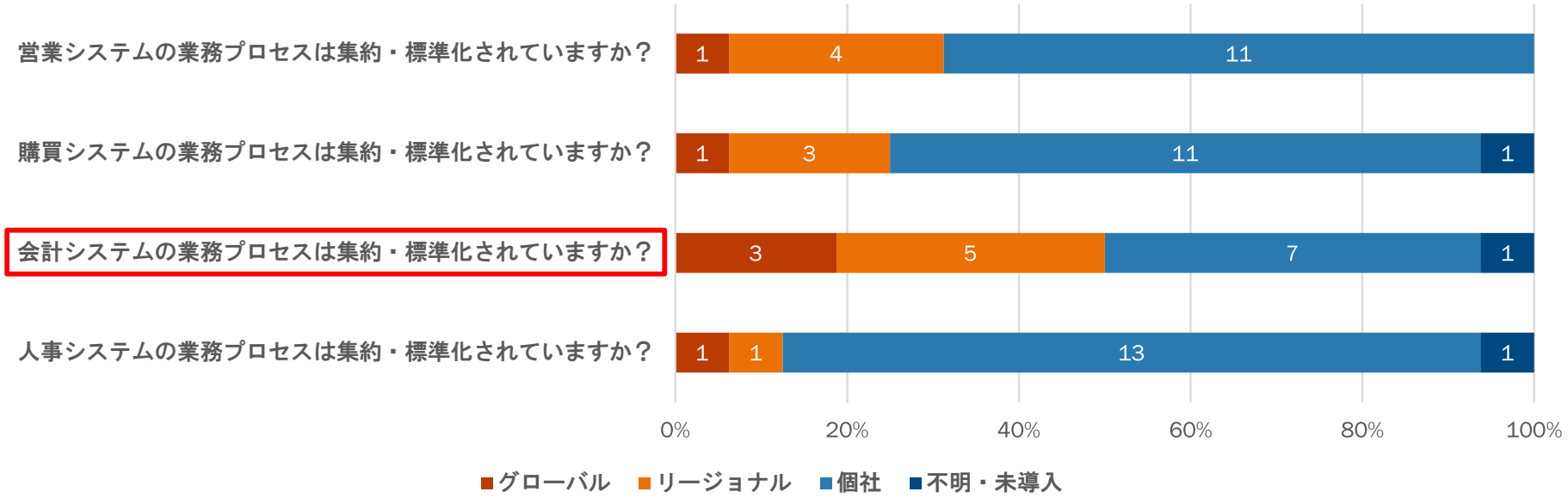
コード体系



コメント

- ERP導入と共にグローバル管理の方向。
- **ERPシステムのリプレイスのタイミングでしか標準化が困難**なため進まない

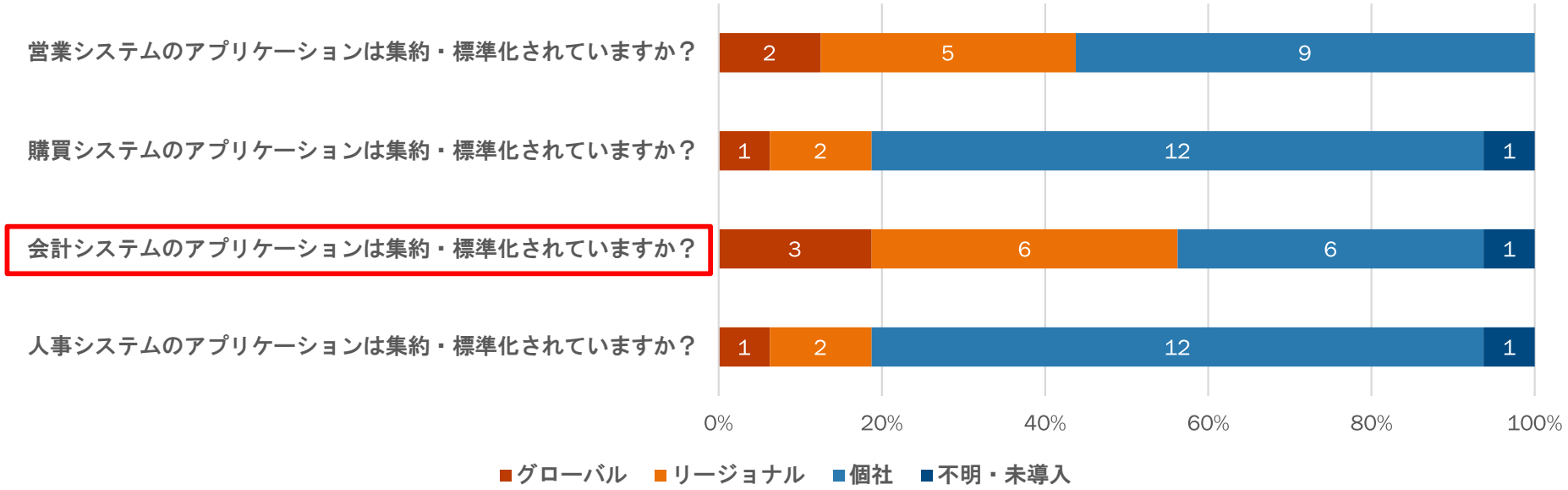
業務プロセス



コメント

- 個別最適化された仕組みが点在し、維持コストUP
- 会社の規模に関わらず、**システムを標準化した場合、費用負担が課題**
- **会社により合弁先も出資比率も製造品種も異なるため標準化に対する強い動機が見当たらない状況**。逆に他社の事例で強い動機があれば参考にさせていただきたい

業務システム・プロセス・コード



コメント

- **<u>各国ルールが異なり、標準化のメリットがないと結論。</u>**
- **プロセスの標準化はあきらめている。会計、人事はパッケージを共通化すれば、ある程度プロセスを標準化できると考えているが、そのインテンションは経理・人事部にはない。その他は、組織体制やビジネスモデルが違うため、<u>労多くして益なしだと考えている。</u>**

全般（標準化を諦めた事例、背景）

- システム構築を先に進めた結果、体制、利活用の共通認識が得れず途中断念。
  - マスターデータマネジメントシステム（体制、ルール整備が必要）
  - CRMの導入（利活用の共通認識合わず）

- 費用対効果
  - 本社標準システムが費用対効果の面で採用されない
  - 各社固有のアンチウイルスソフトの契約からグローバル共通に切替える際に、ライセンス期間が各社と全体で合わず、一部会社が追加負担が必要となってしまった

- 国による法律、規制、商習慣
  - 取引先が共通なのは一部で大部分が各社固有のため標準化のメリットがない
  - ID管理システムにおいてGDPRの関係で個人情報の国外配置が不可

- 本社（日本）主導による標準化の課題
  - 日本側の運用と現地運用でのギャップ（休祝日、言語）

- 1班　システムの標準化およびデータ活用
- **2班　ベンダーマネジメント**
  ・コミュニケーションツール
- 3班　働き方の変化（含むセキュリティ）

2021年度　JUAS グローバルフォーラム 2班

ベンダーマネジメント・コミュニケーションツール

2班メンバー

名前（敬称略）	Company Name
倉島秀典	Mitsubishi Corporation
大洞勝彦	Toray Industries (Malaysia) Sdn. Berhad.
等々力圭史	Idemitsu Asia Pacific Pte. Ltd.
田中正敏 浜田紳之介	Shimadzu (Asia Pacific) Pte Ltd.
大塚隆行	Tokio Marine Asia Pte. Ltd.

Oct 2021

目次

①ベンダーマネジメント

【アンケート分析】

- マネジメント全般
- ITインフラ・セキュリティ
- 業務アプリケーション
- クラウド

②コミュニケーションツール

【アンケート分析】

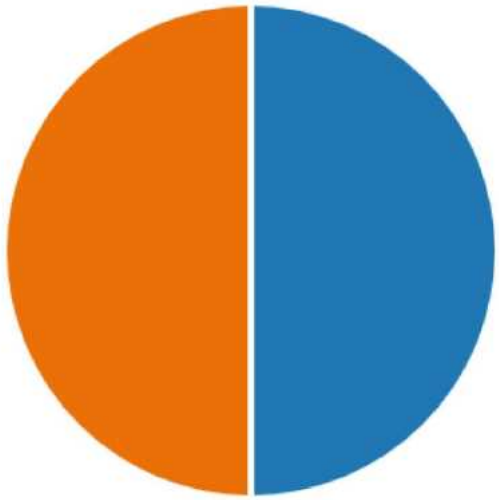
- Teams・Microsoft365全般
- コミュニケーション環境

※ アンケート回答社数：12社

マネジメント全般

3. ベンダー選定・導入・管理に関する社内規程・ガイドラインがありますか。

はい	6
いいえ	6

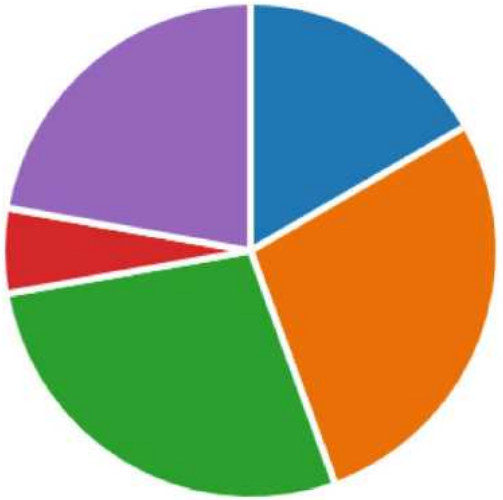


- 半数の会社でルール整備が進んでいる。

マネジメント全般

4. ベンダー選定に日本HQはどの程度関与していますか。（複数選択可）

ガイドラインやルールを統一	3
推奨のベンダーやサービスを予め定...	5
候補の紹介や妥当性を評価する...	5
選定結果を承認する立場にある	1
その他	4



【その他】
- ✓ 内部統制の項目として各社でのルール作成を要請している。サンプルを提供。
- ✓ HQ主導のプロジェクトは、ベンダーは決まっているが、それ以外は各社別。
- ✓ 関与なし。

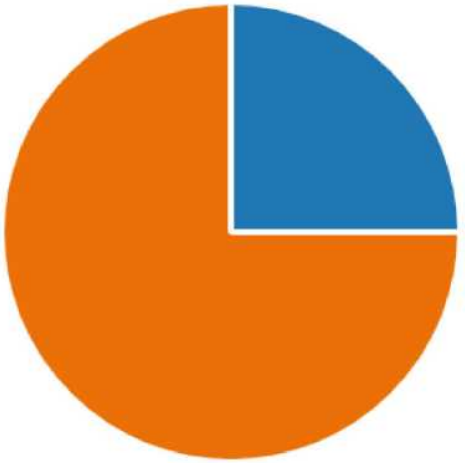
- 8割（10/12社）の会社が何らかの形で、日本HQが関与している。
- ルール整備に留まらず、過半数の会社がベンダー提示や評価など実働レベルで関与。

マネジメント全般

5. 導入フェーズでのベンダー対応まで日本HQがサポート（PMO等）してくれますか。

Insights

はい	3
いいえ	9

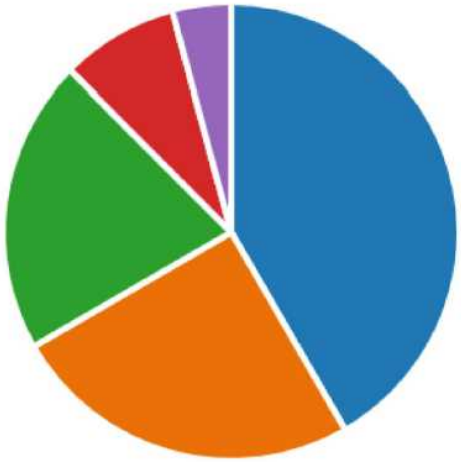


- 工数や期間、物理的な制約も多い導入フェーズまで実働しているのは少数派。

マネジメント全般

6. ベンダーを起用する場合の必要・考慮事項があれば教えてください。（複数選択可）

複数ベンダーによる競争入札を行う	10
決裁できる金額に上限を設けてい...	6
信用調査を行う	5
企業情報（資本金、売上高、社...	2
その他	1



【その他】
✓ **日本HQ提供のチェックリストを用いた確認を実施。**

- **複数ベンダーによる相見積もり**
- **決裁権などコントロールを掛けている会社が半数。チェックリストや企業情報で一定の制約を掛けているケースもある。**

マネジメント全般

7. ローカルベンダーの取り扱いについて以下のいずれが最も当てはまりますか。

Insights

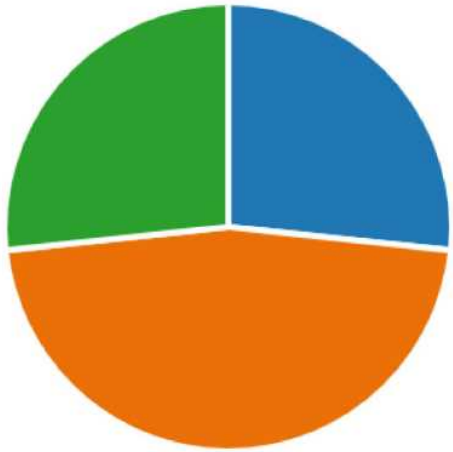
積極的に採用を検討	1
日系やグローバルベンダーを優先的...	4
どちらでもない	7

- 取り扱いに大きな偏りはなかった。
- シンガポールの特性として、ローカルベンダーを特に意識していない？？

マネジメント全般

8. IT全般の対応を包括的に相談・委託するパートナーベンダーがいれば教えてください。
（その他の欄に社名を記入）

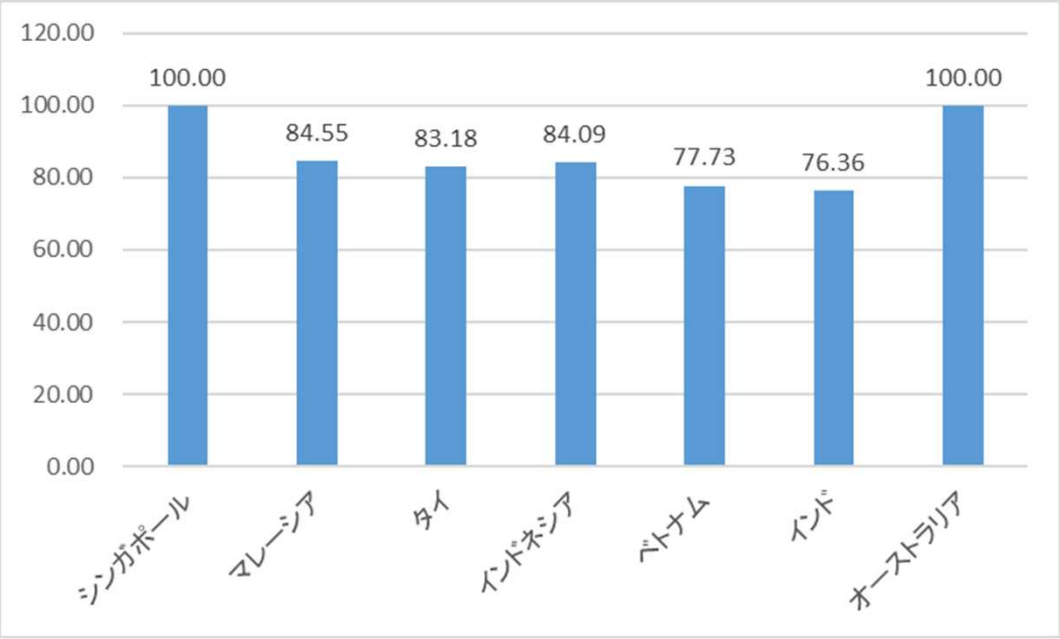
いる	4
いない	7
その他	4



- 案件ごとにベンダーを選定している会社が大半。

マネジメント全般

9 – 14. シンガポールのハードウェア・ソフトウェア価格感を100とした場合、各国の同価格感はどれぐらいの印象ですか。把握している情報や、ご自身の肌感覚に基づきご回答ください。

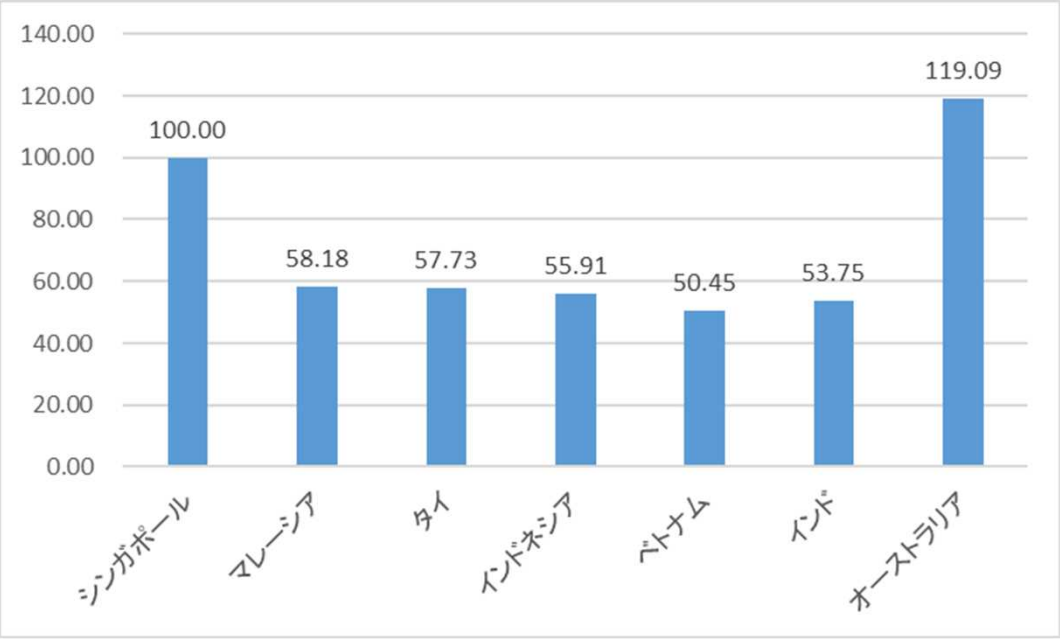


シンガポール	100
マレーシア	100,100,100,100,100,90,80,80,80,50,50
タイ	100,100,100,90,85,80,80,80,70,70,60
インドネシア	120,100,100,100,90,85,80,80,70,50,50
ベトナム	100,100,100,90,80,80,80,75,70,50,30
インド	100,100,90,80,80,80,80,70,70,60,30
オーストラリア	100,100,100,100,100,100,100,100,100,100,100

- マレーシア・タイ・インドネシア　：　83~84%
- ベトナム・インド　：　76~77%
- オーストラリア　：　100%（全社、違いなし）

マネジメント全般

15 – 20. シンガポールのSE単価の価格感を100とした場合、各国の同価格感はどれぐらいの印象ですか。把握している情報や、ご自身の肌感覚に基づきご回答ください。



シンガポール	100
マレーシア	100,80,80,70,50,50,50,50,40,40,30
タイ	100,80,70,70,60,50,50,30,50,40,35
インドネシア	100,80,70,70,50,50,50,50,40,30,25
ベトナム	100,80,70,50,50,40,40,40,40,30,15
インド	100,70,70,70,60,50,50,40,40,35,30,30
オーストラリア	200,130,120,120,120,120,100,100,100,100,100

- マレーシア・タイ・インドネシア・ベトナム・インド　：　50~58%
- オーストラリア　：　120%

PC関連

21. ★★★PC関連★★★

パソコン本体の調達ベンダーは統一していますか？

Insights

日本HQがグローバルで統一	2
RHQが地域内で統一	2
各社ごとに調達	8

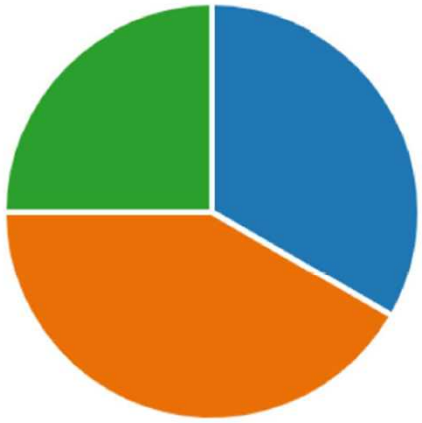
22. パソコン本体の調達先ベンダーを教えてください。（その他の欄に社名を記入）

製造メーカーから直接購入	7	Dell, datadynamics
販売代理店から購入	6	Evotech, NSSOL
その他	4	

PC関連

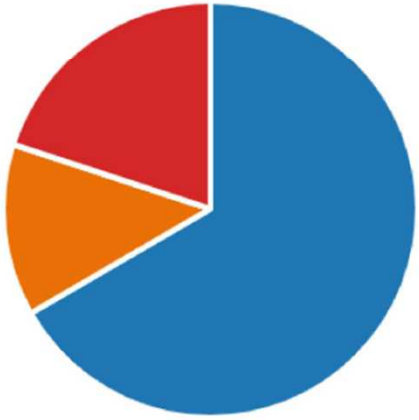
23. パソコン本体の凡その調達価格を教えてください。

～10万円	4
10～15万円	5
15～20万円	3
20万円～	0



24. パソコンのキッティングをベンダーに依頼していますか？　依頼している場合は費用感も教えてください。（その他の欄に社名・費用感を記入）

依頼していない	10
調達ベンダーに依頼	2
別のベンダーに依頼	0
その他	3



- 調達を日本HQかRHQが統一している会社は価格が抑えられている傾向にある
- 販売代理店より購入している場合、製造メーカに比べ調達価格が高い傾向にある
- キッティングを依頼する際の価格感は、5万円/台、420 SGD/PC、ハード料金に含む。日本HQで統一して購入している場合は、キッティングも含めて安値で購入できている

ネットワーク/セキュリティ関連

25. ★★★ネットワーク/セキュリティ関連★★★

ネットワーク機器/セキュリティ機器(F/Wなど)は統一していますか。

Insights

本社がグローバルで統一	1
RHQが地域内で統一	4
各社ごとに選択	7

26. ネットワーク/セキュリティの運用管理はどのレベルで行っていますか？

Insights

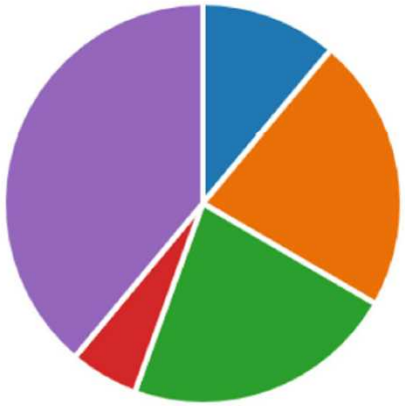
本社が一元的に管理	2
RHQが地域内を管理	2
各社ごとに管理	8

- 機器選定や運用管理を各社で実施しているケースが過半数を超えており、本社が中心となって管理している会社はごく一部。
- 機器選定は本社ではないが、運用は本社から実施しているケースもある

ネットワーク/セキュリティ関連

27. ネットワーク/セキュリティの運用管理をベンダーに委託していますか？　委託していれば社名も教えてください。（その他の欄に社名を記入）

全面的にベンダーに運用管理を委...	2
監視などの定常対応のみベンダー...	4
監視などの定常対応は自社で実...	4
全面的に自社で実施	1
その他	7



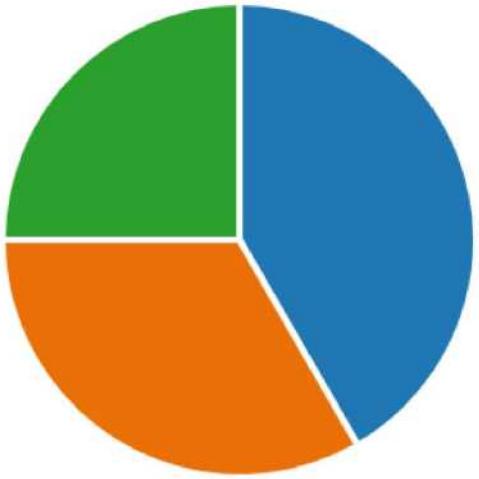
- 「監視：自社、二次対応：ベンダー」と「監視：ベンダー、二次対応：自社」が4社ずつあるのが興味深い。業種での傾向ではなさそう。

会計システム

28. 域内の【会計】システムの導入・運用を主導する組織について教えてください。

Insights

RHQで域内導入・運用	5
各社ごとに独自で導入・運用	4
日本HQから提供されている	3
導入していない	0



【ソフトウェア・起用ベンダー】

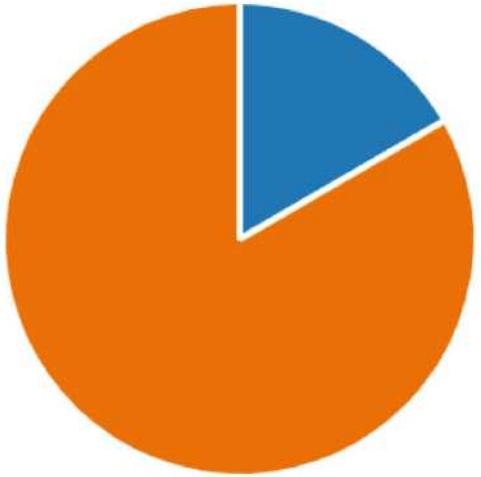
- ✓ SAP
- ✓ SAP
- ✓ SAP S/4 HANA
- ✓ SAP, Tata Consultancy Services Japan
- ✓ SAP（導入コンサルは毎年相見積もりにて評価し、選定している）
- ✓ MS NAV, インドソフトウェア子会社（HQ主導でSAPへ全面入替え中）
- ✓ Oracle
- ✓ Oracle ハイペリオン
- ✓ Oracle ERP
- ✓ EBS, ベンダーはグループ子会社
- ✓ SunAccount
- ✓ 各社毎に選定している

- 日本HQ・RHQ管理で2/3、各社ごとが1/3。
- ソフトウェアはSAPが半数、Oracleも含めると8割。

人事システム

30. 域内の【人事】システムの導入・運用を主導する組織について教えてください。

RHQで域内導入・運用	2
各社ごとに独自で導入・運用	10
日本HQから提供されている	0
導入していない	0



【ソフトウェア・起用ベンダー】

- ✓ SAP
- ✓ SAP
- ✓ SAPサクセスファクター、他(税制、給与計算など地域特性は各社で対応)
- ✓ People Pay, ベンダ：Ascender
- ✓ 自社でQuick HR導入予定（会社はEnable Business Pte Ltd.）
- ✓ 各社様々。Payrollの部分はHRiQ, TalentCloud Ai, BioSoft, HRMS-Pro, EmploymentHero, AllSec Protal, Flex System等。
- ✓ SAGE
- ✓ HRIQ
- ✓ Unit4
- ✓ 自社開発
- ✓ 各社毎に選定している
- ✓ 各社別

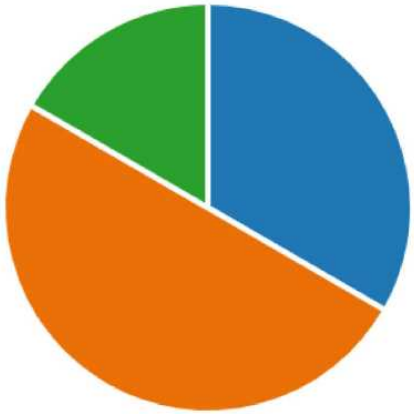
- 8割の会社は各社ごとに導入しており、共通化が難しいことが伺える。
- ソフトウェアはSAPからSaaS、自社開発まで様々。

その他ERPシステム

32. 域内の【ERP（会計・人事以外）】システムの導入・運用を主導する組織について教えてください。

Insights

RHQで域内導入・運用	4
各社ごとに独自で導入・運用	6
日本HQから提供されている	2
導入していない	0



【ソフトウェア・起用ベンダー】

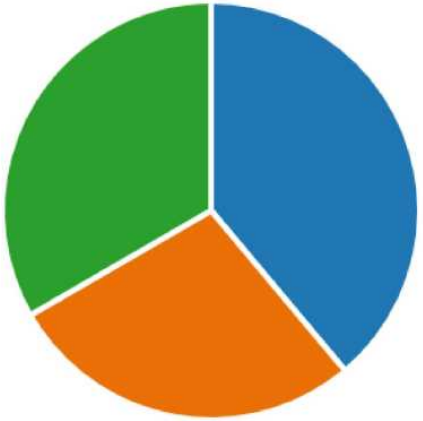
- ✓ SAP
- ✓ SAP S/4 HANA
- ✓ SAP関連が多い
- ✓ SAP, Tata Consultancy Services Japan
- ✓ Policy 400, SAP
- ✓ 現在は自前システム利用。HQ主導でSAPへ全面入替え中。
- ✓ EBS, ベンダー：グループ子会社
- ✓ 自社開発、Oracle
- ✓ マイクロソフト、ダイナミクス365
- ✓ 建設業現場管理ERP、建設業原価管理ERP
- ✓ DXC
- ✓ 特になし。都度選定している。

- 日本HQ・RHQ管理が半数、残り半数が各社ごと。
- ソフトウェアはSAPが半数、Oracle、Dynamics、etc。

業務アプリケーション運用

34. 業務アプリケーションの保守運用・ユーザサポートを外部ベンダーに委託していますか。委託している場合の課題や留意点があれば教えてください。（その他の欄に記入）

はい	7
いいえ	5
その他	6



【その他】
- ✓ 全アプリを同じ外部ベンダーに委託できてない部分もあり、品質面含め標準化ができてない側面がある。
- ✓ 業務プロセスを理解しないまま、ソリューションを提供せずすぐに変更管理に回そうとする。
- ✓ 開発手法の違い、品質管理などに留意している。
- ✓ 時差・祝日対応。
- ✓ グループ子会社に委託。

- 内製化・アウトソースで概ね半々に分かれている。
- 様々なベンダーを国跨ぎで統一的に確り管理することには苦労が多い。

業務アプリケーション導入

35. 各社が個別に業務アプリケーションを導入する場合に、起用ベンダーをRHQでどのように管理していますか。（複数選択可）
管理上の課題や留意点があれば、併せて教えてください。（その他の欄に記入）

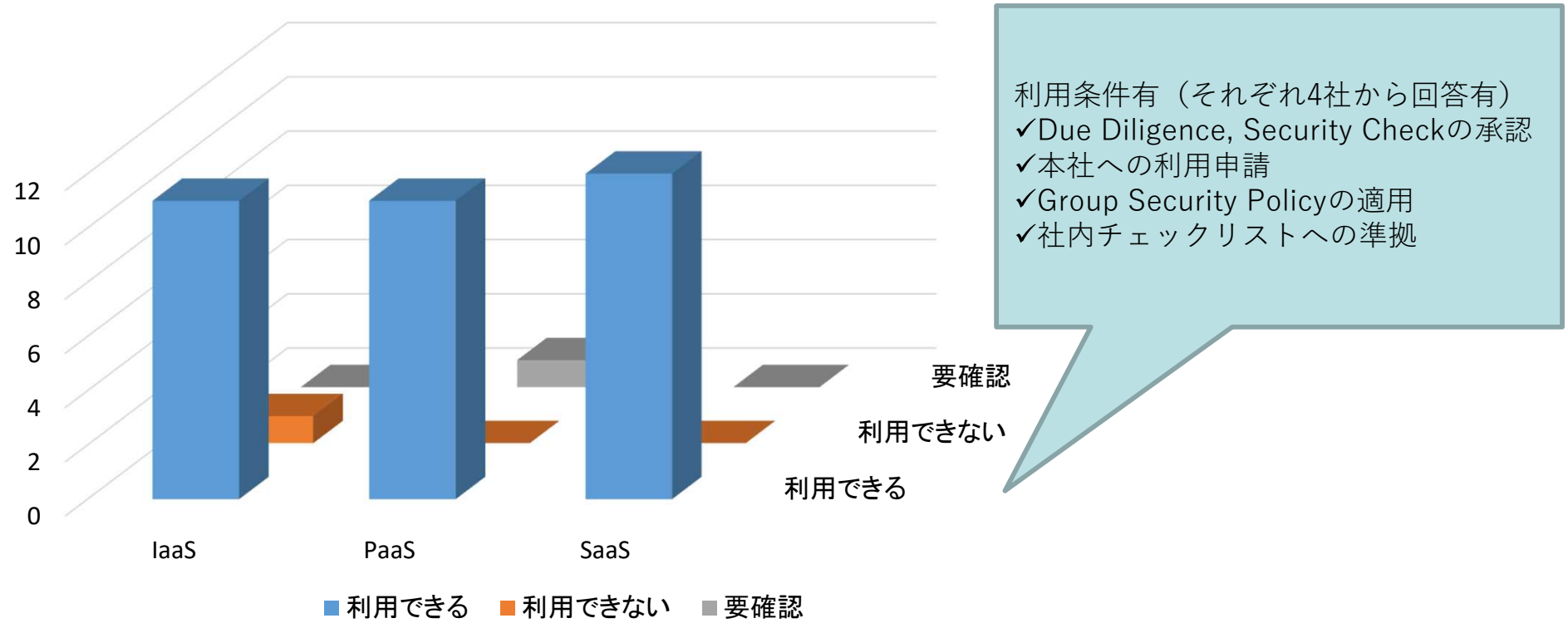
導入時に評価・承認などを行って...	5
導入後の定期モニタリングを行って...	2
各社に任せている	6
各社の独自導入を許可していない	1
その他	5

【その他】
- ✓ **一定額以上の投資はRHQでチェックしている。**
- ✓ **3社相見積もりは取るようにさせている。まずRHQ/GHQから推奨があるか？という問合せが各社から来る。**
- ✓ **本社が各社に対して、年に一度確認する運用としている。（実態は、あまり機能していない）**
- ✓ **毎年、IT投資・MBOにて状況は把握。**
- ✓ **推奨、助言のみ。**

- **約半数の会社が導入タイミングでコントロール（含む決裁権）を掛けている。**
- **各社に任せている場合も、アドバイスやモニタリングで一定の状況把握を実施。**

クラウド

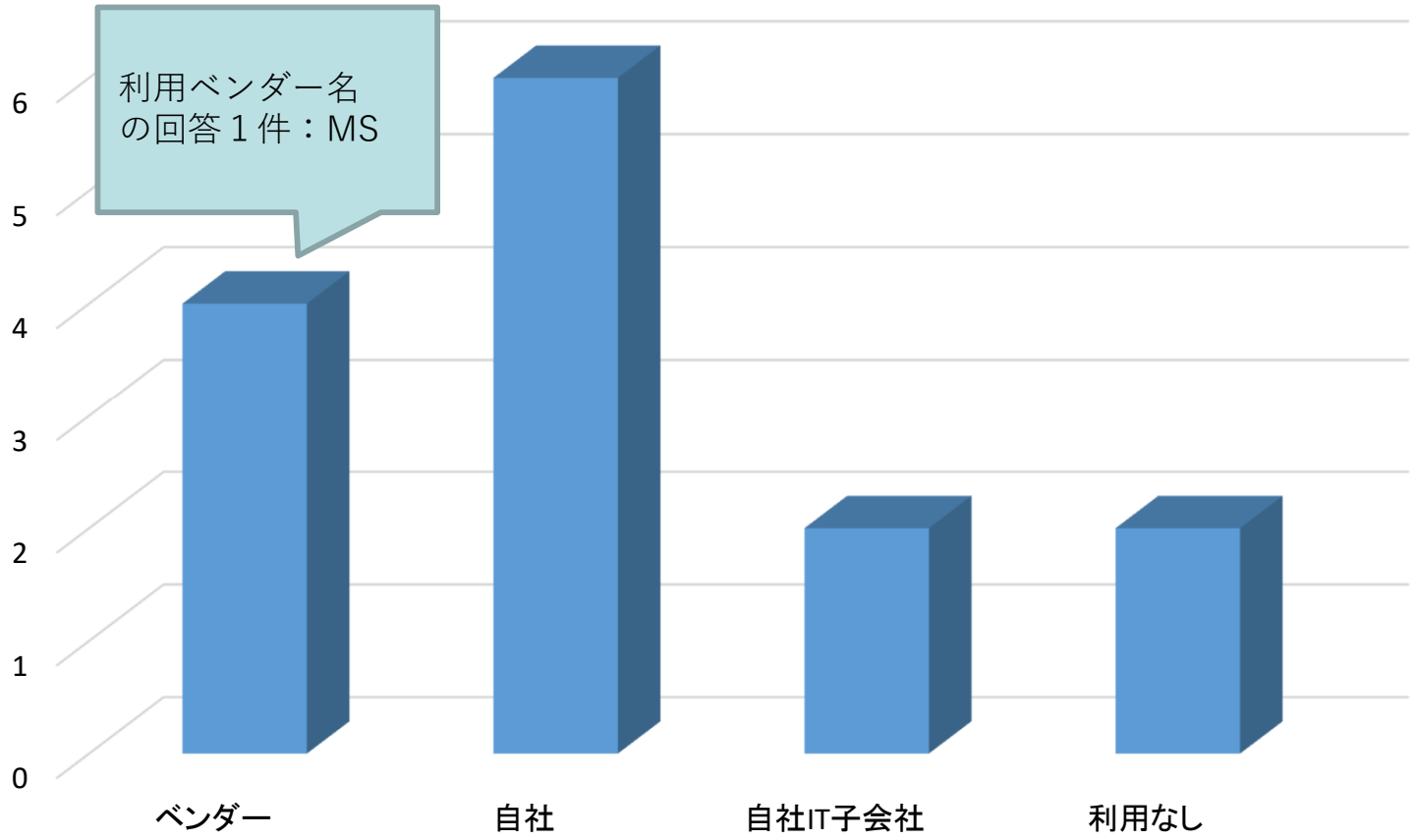
36-38. 【IaaS】 【PaaS】 【SaaS】の利用は可能ですか。 利用する場合の条件があれば教えてください。（その他の欄に記入）



- SaaSは全ての会社が利用可。IaaS、PaaSもほとんどの会社が利用可。
- ベンダーやセキュリティのチェックと承認、本社申請、セキュリティポリシー適用といった利用条件を設けている会社が4社あり。

クラウド

39.　IaaSやPaaSのセットアップは誰が実施していますか。



- 半数の会社が自社でIaaS・PaaSのセットアップを実施。
- 次に多かったのがベンダー利用。

クラウド

40-42.【 IaaS】 【PaaS】 【SaaS】の利用事例を教えてください。

【 IaaS】	【PaaS】	【SaaS】
▪ 富士通社のIaaSサービスとAWSを利用 ▪ AWS、MS Azureクラウドサーバー構築　社内・社外両用 ▪ AWS: オンライン保険販売システムの基盤 ▪ 社内オンプレサーバーのクラウドへの移行など ▪ モバイルAppや代理店向けCRMシステムなどの外部向けシステムのサーバー環境として利用 ▪ 各種業務システム	▪ AWS ▪ 販売管理システムをAWS上に構築予定 ▪ 原価管理システム ▪ Microsoft365(SharePoint. Power Apps, Power Automate)	▪ O365 ▪ M365　コミュニケーションツール ▪ 会計システム（SAP）で対応していない経費精算の処理にProMaster（豪）を利用している。 ▪ KINTONE, KING of TIME ▪ 音声認識文字化（議事録作成支援）ツール、名刺管理ツール、等 ▪ Office 365 ▪ 業務アプリケーションの標準化、自動化など ▪ 人事システム、課題管理システムなど ▪ MS365、HRシステム、ITインベントリ管理システムなど ▪ MS Power BI（データ分析・レポーティング）MS DevOps（開発環境ツール）Merimen（損害保険のクレームシステム） ▪ Microsoft365(Outlook, Teams)

クラウド

43-45. クラウドサービスのガバナンス、クラウドサービス採用にあたり注視している法規制・当局申請、クラウドサービス利用上の課題は？

ガバナンス	法規制・当局申請	クラウド利用上の課題
▪ 上記記載のIaaS,PaaS,SaaSはHQ主導で導入している場合が多いです。その他利用者、金額含めて規模が小さいサービスは個別判断となっています。 ▪ 日々改善中。IT BCP観点で管理中。 ▪ IaaS,PaaSは現時点では利用しておらず、SaaSに特化して、チェックリストの準拠しているサービスかどうかRHQで確認した上で、承認している。 ▪ SAAS 個社で実施PAAS 導入時にHQに相談 ▪ 本社にてガイドラインを作成中 ▪ クラウドサービスセキュリティチェックリストを運用している ▪ 国の当局規制準拠、導入前のDue Diligence, Security Checkのスキームで運営 ▪ クラウド利用ポリシーなどをグローバル、リージョナルで決めている ▪ クラウド利用時に本社へ利用申請を行うことで本社のガバナンスがきくようになっている ▪ HQで用意されたクラウド契約チェックリストを各国へ配布 ▪ HQ提供のクラウドリスクアセスメントシートの起票および承認 ▪ "Microsoft365 は、本社が利用を推進。その他は各地域で基準を作成し導入。基準は本社に提出している。"	▪ 東南アジアでは特になし。GDPRや中国系の話が出てくると検討しているところはあったはず。オーストラリアもオーストラリア内のデータセンターである必要があった。 ▪ 各国の個人情報保護法 ▪ 特になし ▪ データローカライゼーション ▪ 国によってデータの国外保存ができないケースがある ▪ 個人情報保護、情報の国外持ち出し禁止など ▪ 個人情報保護・データ域外移転・所管省庁のシステムリスク管理ガイドライン	▪ 例えば、Azureサーバーを構築したいと思った時。GHQ日本が管理者権限を持っているので、日本に依頼→リードタイム→構築、という思ったより時間がかかること。クラウドのメリットが活かせていない。その後の運用の権限はリージョンにあったりする。 ▪ ローカルベンダーのSaaSはセキュリティレベルが低く、チェックリストに準拠していないケースが多い。 ▪ メインベンダーがノータッチとなるため、総務系SAASの場合総務担当者の負荷（不具合対応等）が高くなる懸念がある。 ▪ クラウドに精通した人財の確保 ▪ コストは安くない、社内技術者の不足など ▪ SaaSシステムは、ICTのサポートなく事業部とベンダーで簡単に導入できるので、ICTで導入の把握が困難。※今は、契約時のW/Fで必ずICTを通るようになっているので、確実に把握可能となった。 ▪ アクセス元制御、アカウント管理、シャドーIT対策 ▪ 知識・スキル不足、法規制対応、リスクアセスメントロード ▪ インタフェースの有無、Oracle使用有無によりクラウド。オンプレミスを切り分けているが、判断が難しいものもある。

クラウド

参照： データの国外持ち出し規制

Impact to use Cloud Services hosing out of the country.

Learn more about countries with data residency regulations by clicking the map

参考文献： Data Residency and Data Localization Research - InCountry

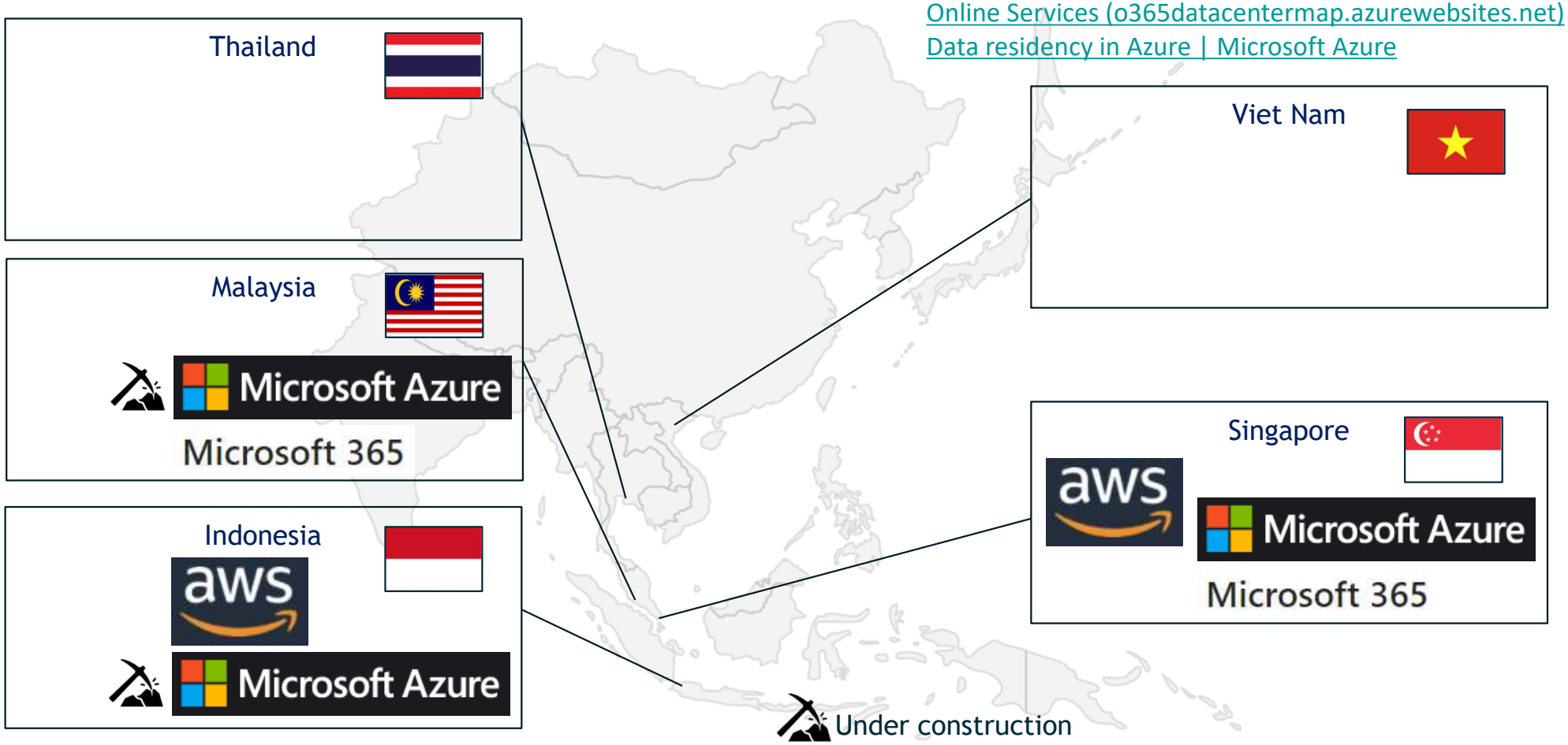
SG	Data Controllers can transfer personal information only to other countries with adequate data protection laws.
MY	Data residency effectively required. A Data Controller may only transfer personal information to countries on a Malaysian government's approval list. However the list has never been officially published.
TH	Data Controllers can transfer personal information only if the other country has adequate data protection laws.
IND	Data residency required. Banks are required to maintain datacenters incountry.
VT	Data residency effectively required. All online service providers have to store, analyze, and process personal data of Vietmanese locally.

クラウド

参照： クラウドデータセンターの状況SEA（Azure、AWS、M365）

Need to follow up with the DC status of Cloud Services.

Global Infrastructure (amazon.com)
Online Services (o365datacentermap.azurewebsites.net)
Data residency in Azure | Microsoft Azure



クラウド

参照： クラウドに関する直近の金融監督当局規制

Singapore (MAS) 2021/3	Malaysia (BNM) 2019/6	Indonesia (OJK) 2021/4
ADVISORY ON ADDRESSING THE TECHNOLOGY AND CYBER SECURITY RISKS ASSOCIATED WITH PUBLIC CLOUD ADOPTION	Risk Management in Technology (RMiT)	Placement of Electronic Systems at Data Centers and/or Disaster Recovery Centers
Request a comprehensive risk assessment for public cloud adoption and appropriate management for identified risks. 1. Developing a public cloud risk management strategy for IaaS, PaaS and SaaS respectively. 2. Implementing strong controls in areas such as IAM, cyber security, data protection and cryptographic key management 3. Expanding the FI's cyber security operations to include security of public cloud workloads 4. Managing cloud resilience, outsourcing, vendor lock-in and concentration risks 5. Ensuring FI's staff have adequate skillset to manage public cloud workloads and risks.	Financial institution is required to conduct a comprehensive risk assessment prior to cloud adoption which considers the inherent architecture of cloud services that leverages on the sharing of resources and services across multiple tenants over the Internet. Financial institution is required to consult BNM prior to the use of public cloud for critical systems, and to notify to BNM for non-critical systems.	Non Bank FIs that have Data Centers and/or Disaster Recovery Centers are required to place Electronic Systems at Data Centers and/or Disaster Recovery Centers in Indonesian territory. Non Bank FIs are prohibited from placing Electronic Systems in Data Centers and/or Disaster Recovery Centers outside the territory of Indonesia unless they have obtained approval from the Financial Services Authority.

参加メンバー意見交換

1. ベンダーマネジメント

・グローバルで横断的にみる組織を立ち上げた
・インドIT会社Tataをマネジメント：データセンター管理→横展開、対象拡大、費用感 ○（SIN対比7～80）、品質 △
・オフショア活用の可能性を確認
・インド系ベンダーは要件を聞き入れにくく使いにくい
・品質の低いベンダーを他国で起用するケース、フォローアップに苦労している
・工数の確認にフォーカス、単価は各国ごとの目安を内部で確認
・HKGの子会社に提案依頼して出てきた金額をベンチマークとし、それより安価な場合は、提案不備がないかを確認

2. ネットワーク

・通常の運用は、グローバルネットワーク：NTT、ローカルネットワーク：ネットマークス
・スポットの案件は、１社に集中するとコストの妥当性が分からなくなるので複数社見積する
　→ 複数社見積で必ず安くなるとは限らない、自社の想定する作業範囲が適切かどうか
　　複数社だと違う視点で提案が出る、納期に差がある

3. マネージドサービス

・NTT（ネットワーク、セキュリティ）、富士通（運用）を起用
・人が変わるとサービスレベルが変わる（日本人出向者の質も変わる）
・委託先の担当者が他の会社に移ると、移った先の会社に契約を変えることもある

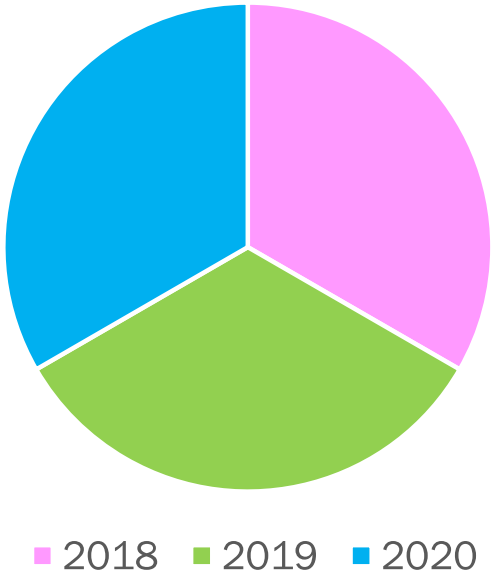
4. 日系企業のメリット

・日本人がいる会社がよいとは限らない
・金額は機器や導入先の国によって異なる
・契約形態は基本的には日本と同じ、準委任の案件が日本より少ない印象

コミュニケーションツール（Teams）

46. ★★★コミュニケーションツール関連★★★

Teamsの導入時期を教えてください。



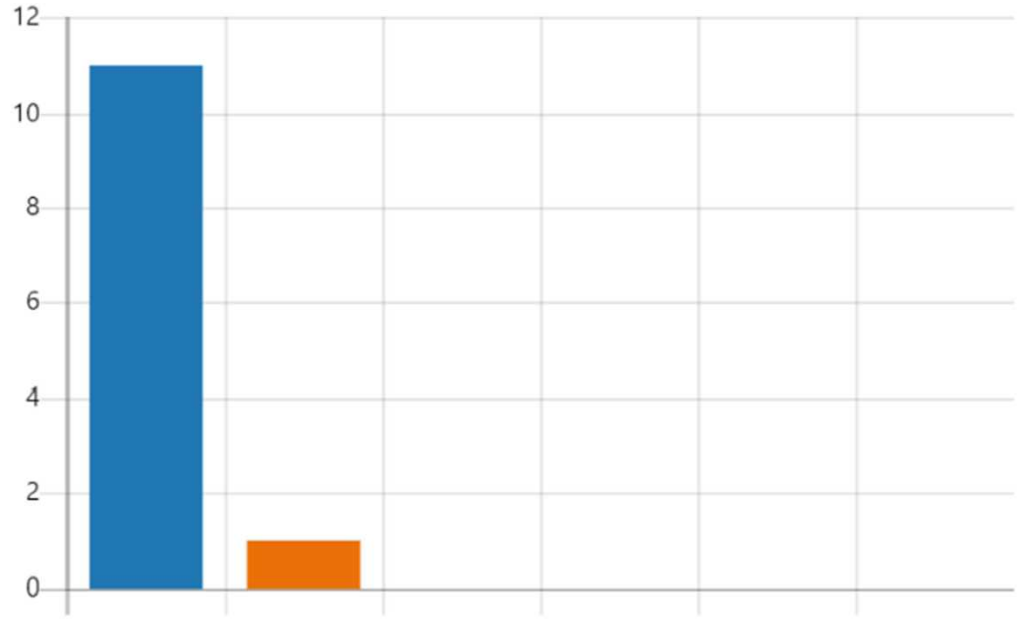
- 導入時期にバラつきはあるが、参加企業は全てTeams導入済
- 2020年5月導入が最遅（各社、導入から1年半経過）
- 本社導入の一年後に海外導入したという企業もあり

➡導入時期は、以降の回答に、それほど大きな相関関係なし

コミュニケーションツール（Teams）

47. 全ユーザのうち、どの程度がTeams（というコミュニケーションツール）自体を認識していると思いますか。

90%以上	11
75~90%	1
50~75%	0
25~50%	0
0~25%	0
不明	0



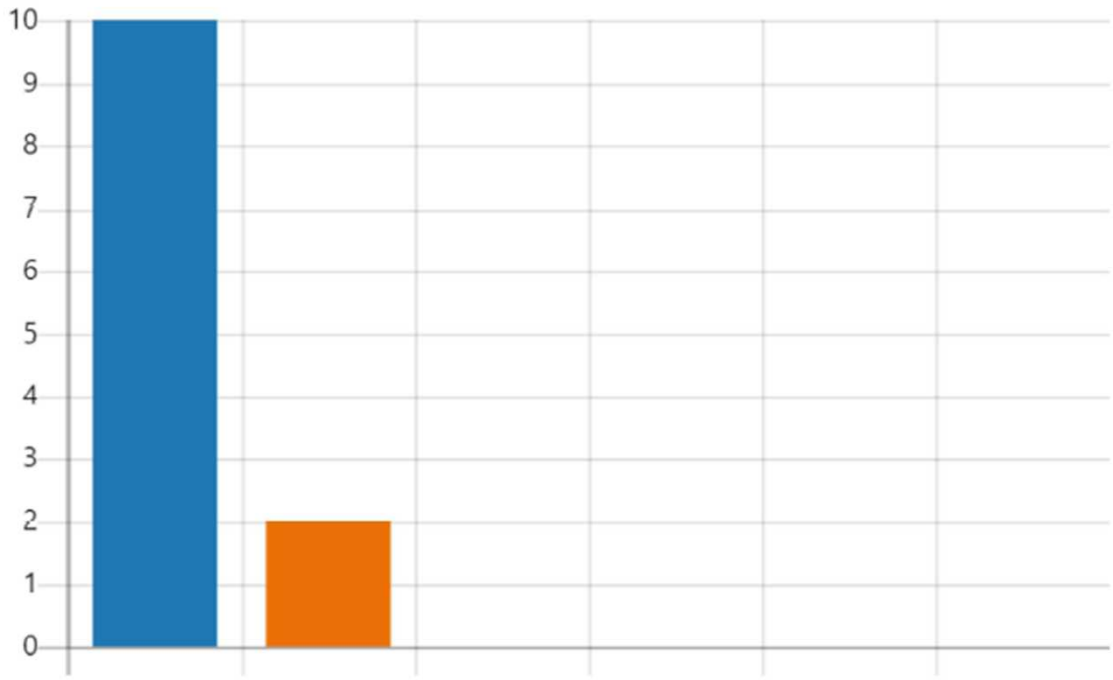
- ほぼすべての企業・ユーザがコミュニケーションツールとして認識している
- 75-90%以上の1社は、2018年導入（導入時期だけの問題ではない）

コミュニケーションツール（Teams）

49. 全ユーザのうち、どの程度がTeamsの【Web会議】機能を利用していると思いますか。

Insights

90%以上	10
75~90%	2
50~75%	0
25~50%	0
0~25%	0
不明	0



- TeamsのWEB会議は、ほぼすべての企業・ユーザが利用している

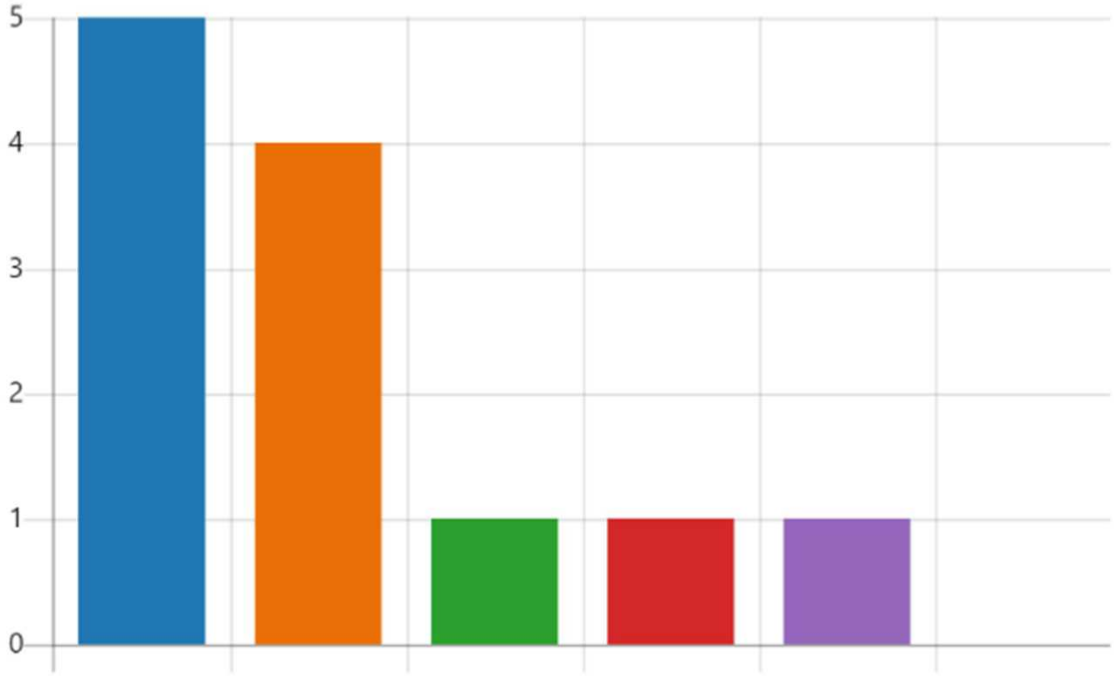
➡コロナ影響もあり、利活用が進んだのでは（今や必須ツール/スキル）

コミュニケーションツール（Teams）

48. 全ユーザのうち、どの程度がTeamsの【チャット】機能を利用していると思いますか。

Insights

90%以上	5
75~90%	4
50~75%	1
25~50%	1
0~25%	1
不明	0

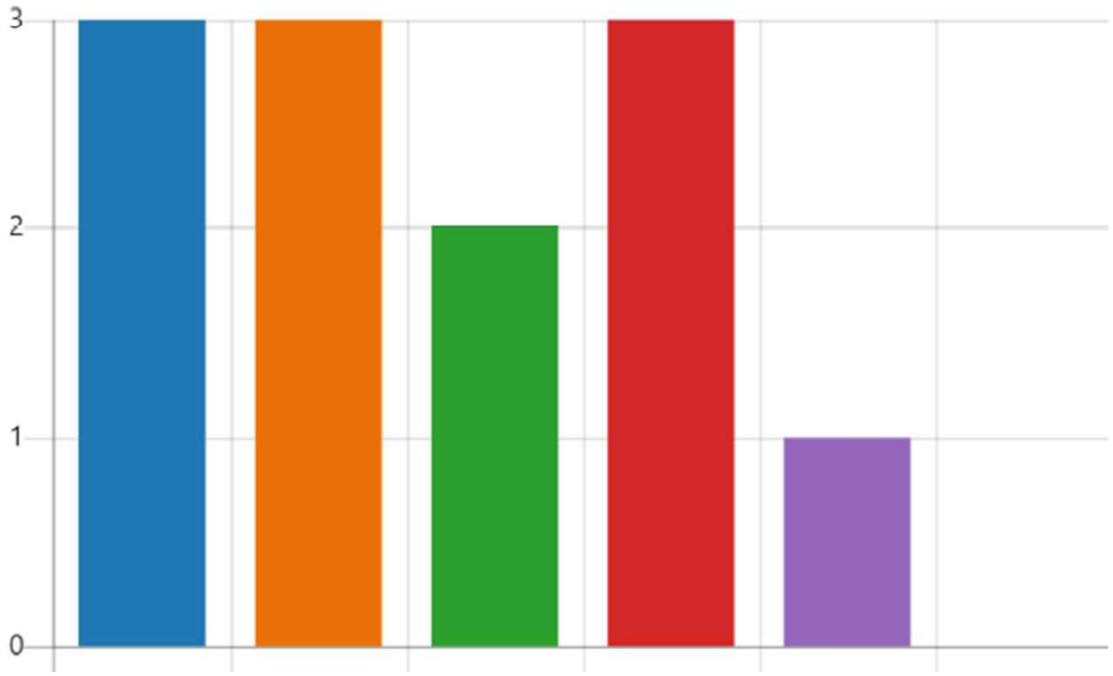


- 過半数の企業・ユーザは、Teamsチャットを利用している
- Web会議機能と比べると、利用率は劣る

コミュニケーションツール（Teams）

50. 全ユーザのうち、どの程度がTeamsの
【チーム（メンバ限定グループチャット）】
機能を利用していると思いますか。

90%以上	3
75~90%	3
50~75%	2
25~50%	3
0~25%	1
不明	0



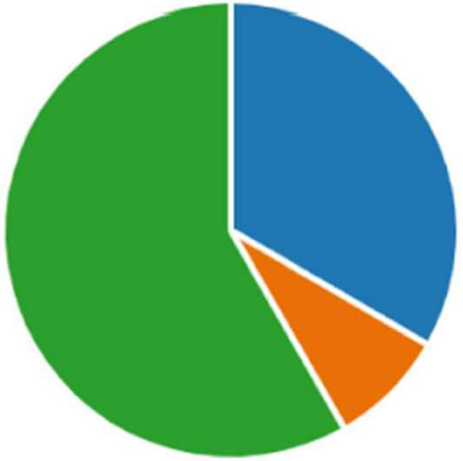
- チーム（グループチャット）機能は、WEB会議ほど利用されていない
- チャット浸透75%超企業でも、内2割はチーム未浸透

➡ ユーザ教育の実施有無、OutlookやSlack等、他ツールとの使い分けの問題もあると考えられる

コミュニケーションツール（Teams）

51. Teamsのチーム登録権限の運用について教えてください。

一元管理（IT部門にのみ登録権限あり、IT部門が各部署からの申請に基づいて作成する等）	4
組織ごとに管理者を設け、管理者によって登録する	1
制限していない（全ユーザがチームを登録できる）	7



- **過半数の企業は、チーム登録に制限をかけていない**
- **前ページ（グループチャット機能利用率）で75%以上と答えた会社のうち過半数が「制限していない」と回答**

➡チーム登録権限（制限）の有無も、Teamsの利活用に寄与している

コミュニケーションツール（Teams）

52. Teamsの管理について、課題認識していることがあれば教えてください。

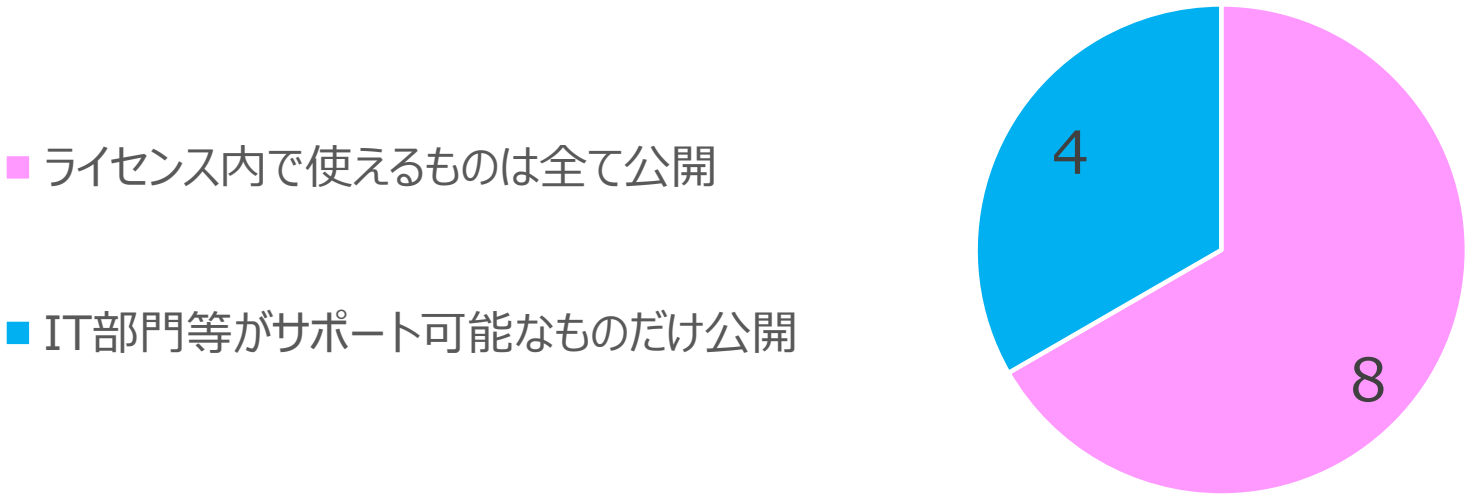
- 管理者退職時の運用が未定
- チーム乱立（どこに何の情報があるかわからない、不要チームの棚卸ができない）
- 異なるテナントおよび社外とのコミュニケーション時の利便性の低下
- 海外拠点においてはWEB会議ツールとしてしか認識されていない（周知活動の必要性がある）

➡利用者およびチームの拡大に伴い、徐々に運用面での問題が浮き彫りになりつつある。しかしながら、Teams利用に影響をきたすほどの大きな課題にはなっていない。

人事情報に紐づくメーリングリストをチーム参加者に設定して異動時に自動で権限付与されるようにする、不要なチームの運用方法を定める等、IT担当によるルール作り・継続的な改善対応が必要になると考えられる

Microsoft 365アプリケーション

53. Microsoft365の各アプリケーション利用に関するシステム制限（ユーザへの公開有無）の考え方を教えてください。

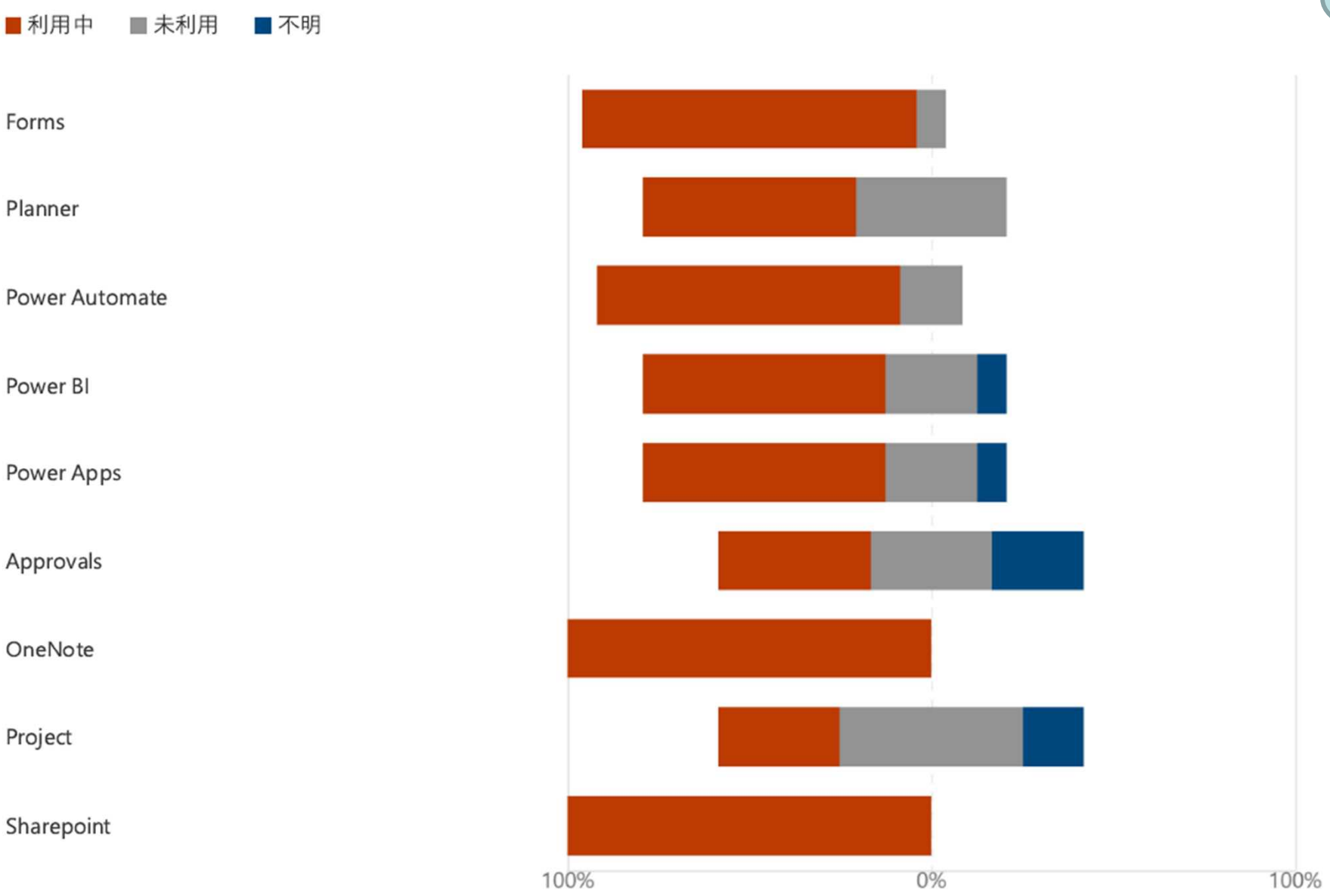


- **3割は、セキュリティ面/ユーザサポート面を考慮して、機能制限している**

Microsoft 365アプリケーション

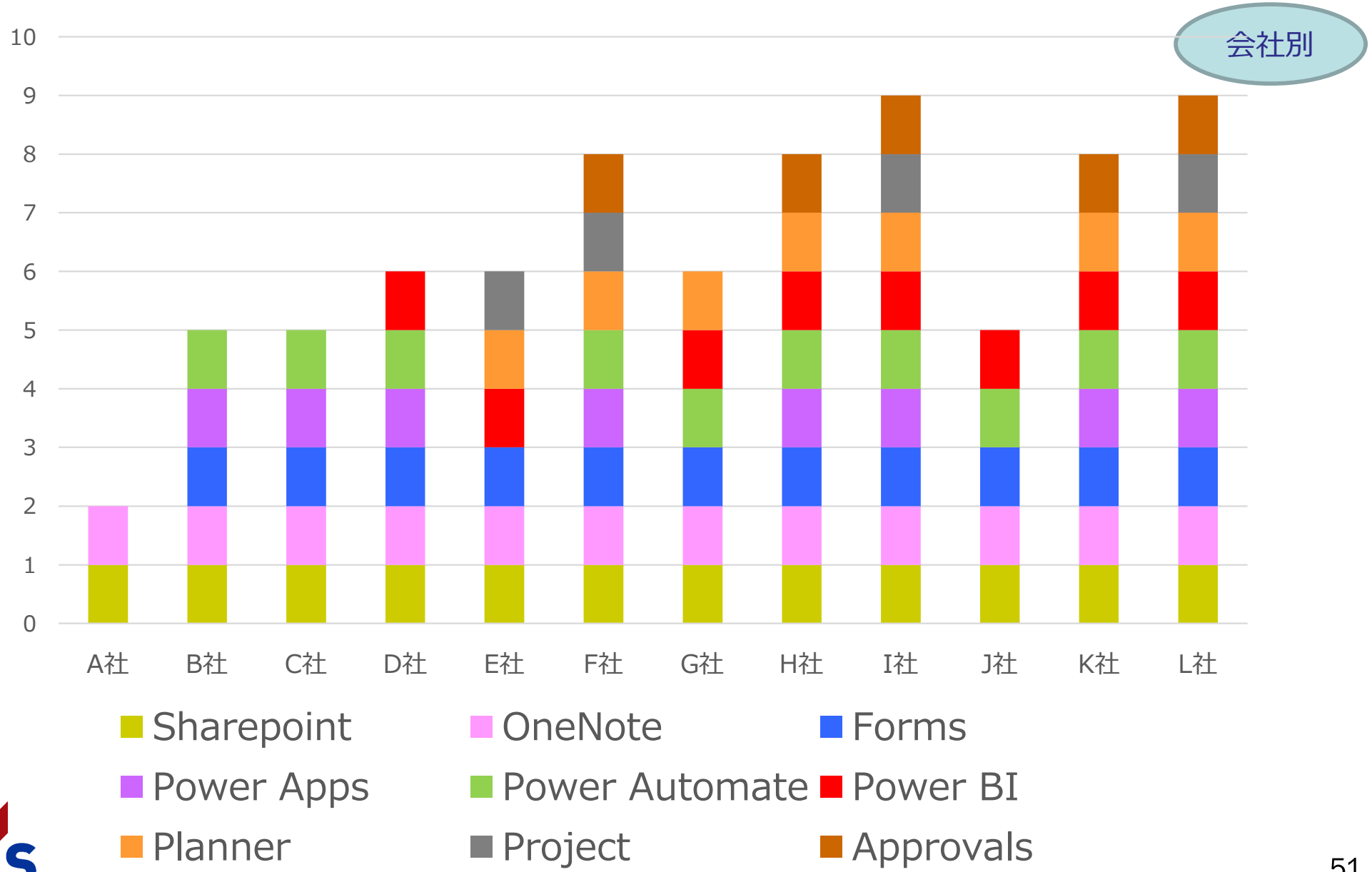
54. Microsoft365の以下アプリケーションの利用状況を教えてください。

アプリ別



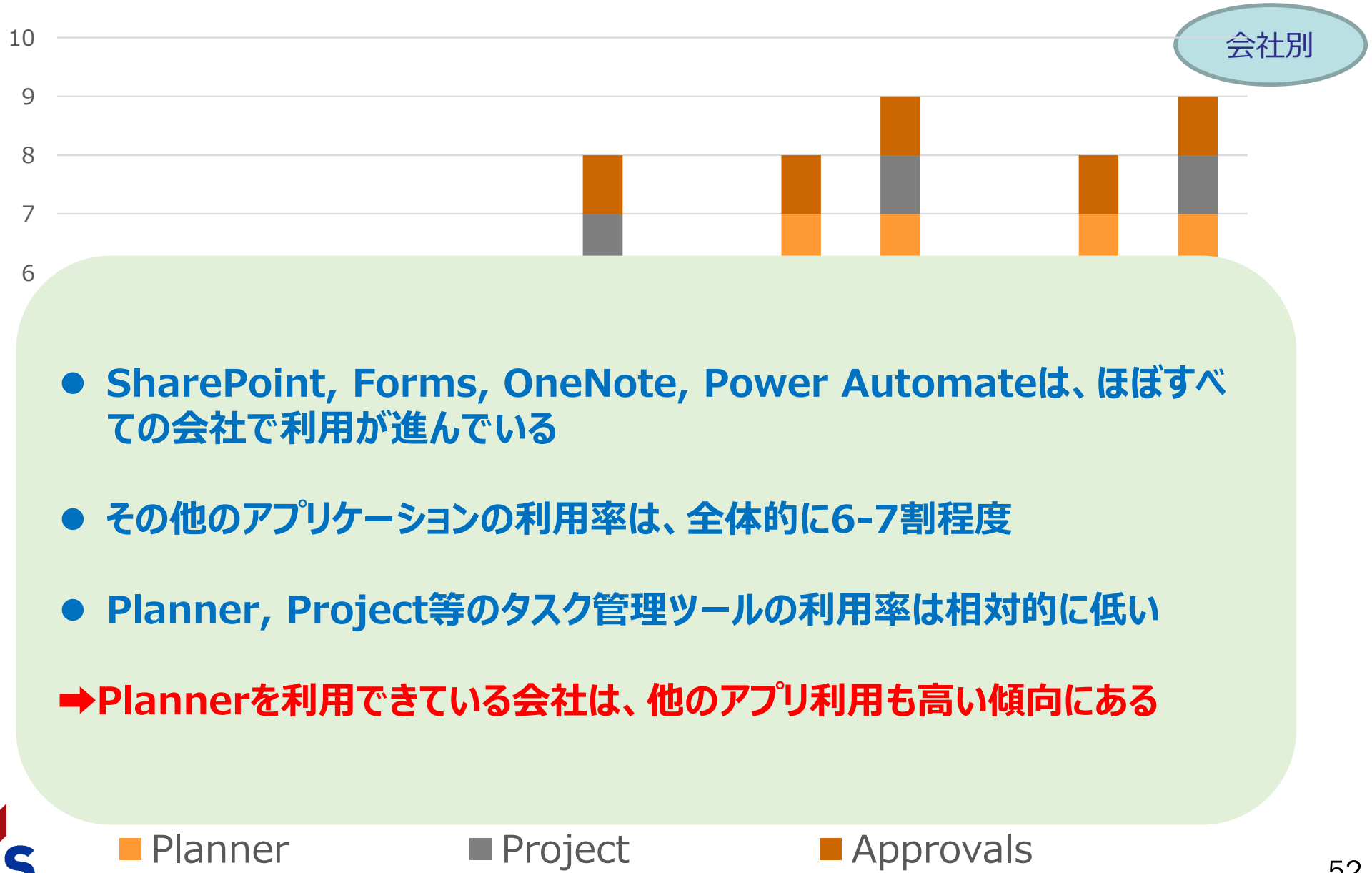
Microsoft 365アプリケーション

54. Microsoft365の以下アプリケーションの利用状況を教えてください。



Microsoft 365アプリケーション

54. Microsoft365の以下アプリケーションの利用状況を教えてください。



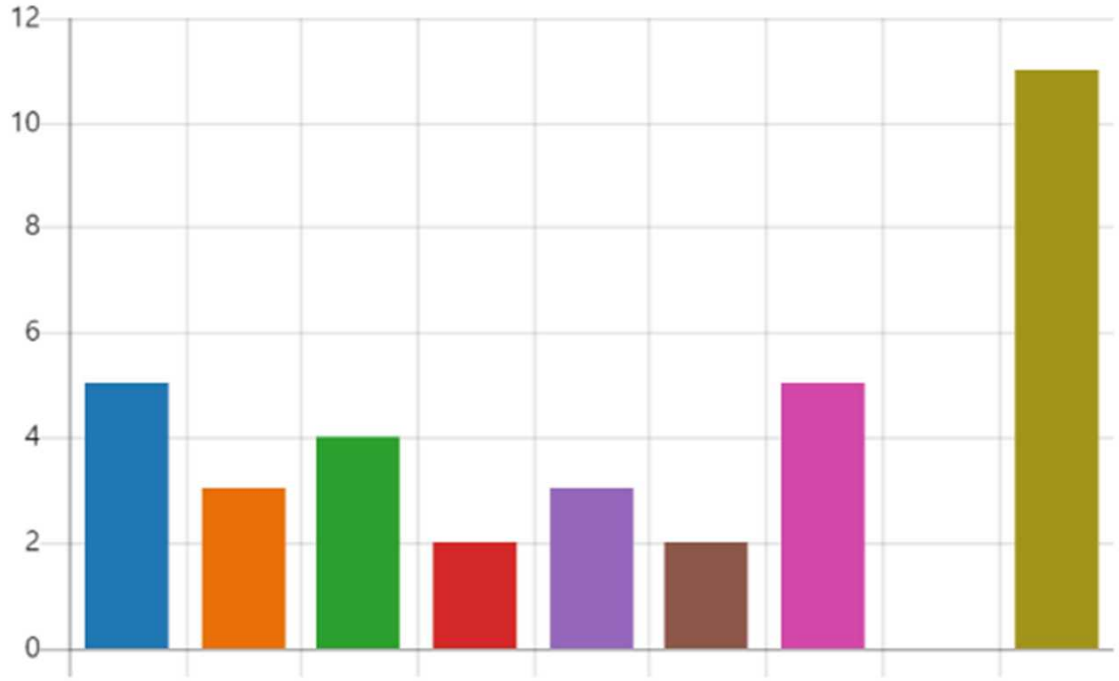
- **SharePoint, Forms, OneNote, Power Automateは、ほぼすべての会社で利用が進んでいる**
- **その他のアプリケーションの利用率は、全体的に6-7割程度**
- **Planner, Project等のタスク管理ツールの利用率は相対的に低い**

➡Plannerを利用できている会社は、他のアプリ利用も高い傾向にある

Microsoft 365アプリケーション

55. IT部門として積極的に活用推進した（ユーザへ操作説明、利活用に向けてテンプレート構築・展開など進めた）アプリケーションがあれば教えてください。（複数選択可）

Forms	5
Planner	3
Power Automate	4
Power BI	2
Power Apps	3
Approvals	2
OneNote	5
Project	0
Sharepoint	11

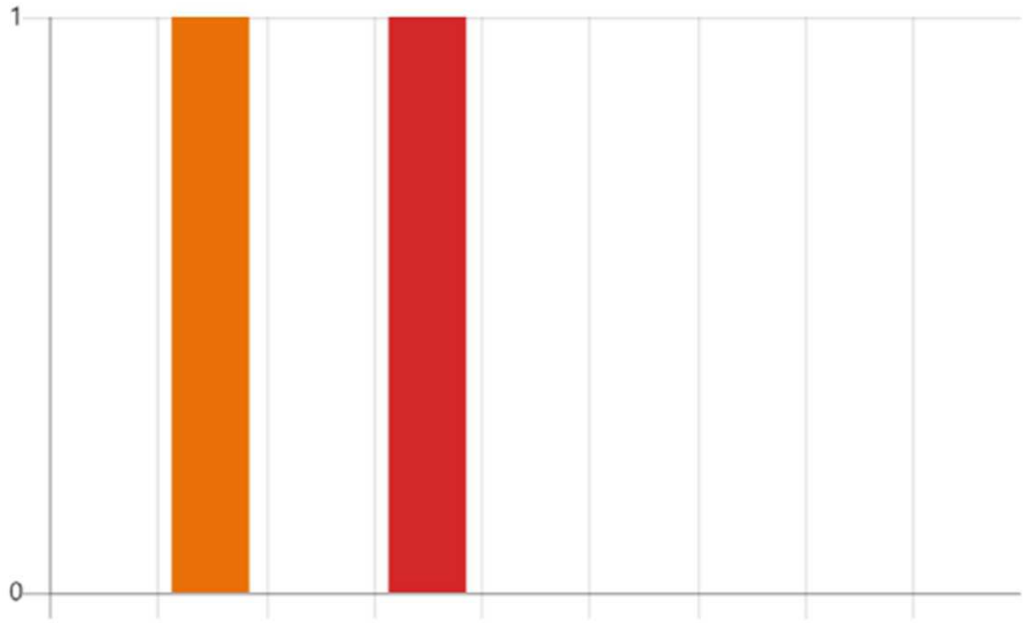


- SharePointは、ほぼすべての会社でIT部門から活用推進済
- OneNote, Formsは、およそ半数の会社で、IT部門から利用促進中
- その他のアプリケーションの推進率は2-3割程度

Microsoft 365アプリケーション

56. 上記55で活用推進したものの、課題が発生し展開を諦めたアプリケーションがあれば教えてください。（複数選択可）

Forms	0
Planner	1
Power Automate	0
Power BI	1
Power Apps	0
Approvals	0
OneNote	0
Project	0
Sharepoint	0



- 前ページと比較すると、どの会社もそれほど大きな課題には直面していない
- PowerBIは、IT部門が現場に刺さるイメージができず、WEB化するためには有償ライセンスであること、他ツールに比べ説明時間（操作習熟の為の時間）も必要という背景があり、勉強会そのものの企画立案に苦戦中
- Plannerは、タスクの順序関係を管理できない、EXCELの列追加ほど自由に属性項目追加ができない、外部ベンダーが参照しにくい等の理由で大型プロジェクトのタスク管理には不向き（Excelの方が良かった）と判断

Microsoft 365アプリケーション

57. Microsoft365アプリケーション・全般ツールに関して、成功事例・失敗事例・教訓・注意事項等があれば教えてください。

＜課題＞
- 導入後のネットワーク負荷が試算していたよりも高く、展開先会社で回線増速が必要になることが多い。
- 完全にユーザーツールの扱いとしているため、利活用推進ができていない
- マニュアルやガイドラインFAQが揃えられていない
- 本社主導での展開は、期待できないため、各店での意思決定・展開推進が必要

＜成功例＞
- SAPの課題チケット管理システムを作ることができた
- Power Automateを利用したWorkFlowを構築し、Papreレス活動を推進した
- Power Platformを活用して経理伝票のデジタル回付アプリを作成・導入して社内のペーパレス化が進んだ。
- 日本ではパソコン入替と合わせてTeams展開したため、そのタイミングでユーザ説明会を実施し活用推進しつつ使いこなし講座という誰でも参加できる講座を定期開催しフォローアップを実施

コミュニケーション環境

58. 全社内とコミュニケーションを図るために、どのようなツールを使っていますか。
（例）Sharepointにて全社ポータルを作成している　等

12
応答

最新の回答

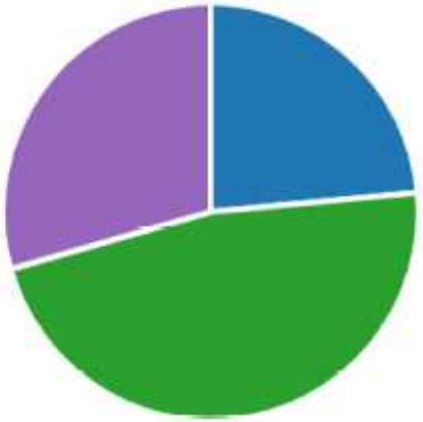
"Sharepointにて全社ポータルを作成している"

"Outlook 全社員向けemailとTeams での全社MTG（Townhall）"

"・SharePointにてポータルサイトを作成している。"

59. 社外とのデータ共有にどのようなツールを利用されていますか。（複数選択可）

BOX	4
Google Suite	0
OneDrive+Sharepoint	8
指定なし（Free Strage等で運用...	0
その他	5

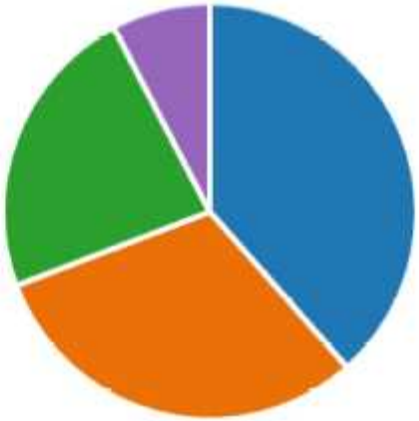


- ここまでの質問でも、SharePointの活用推進を進めている会社が多いという結果だったが、社内・外のデータ共有にSharePoint（およびOneDrive）を利用している会社が多い。また、ほぼすべての参加会社で社内ポータルが活用されている。
- 社外との共有では、BOX以外には「宅ふぁいる」、「TBOX」の利用事例あり。

コミュニケーション環境

60. 在宅勤務時など事務所外からコミュニケーションツールを使うときの手段について教えてください。（複数選択可）

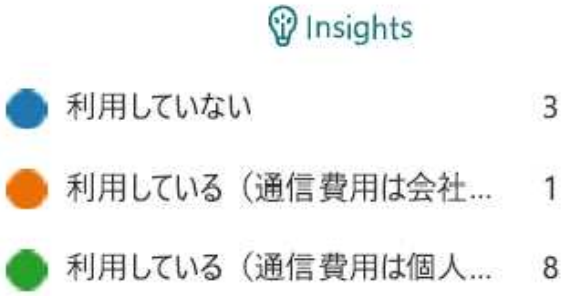
VPN	10
MDM（Intune等）	8
Two-factor authentication (2FA)	6
許可していない	0
その他	2

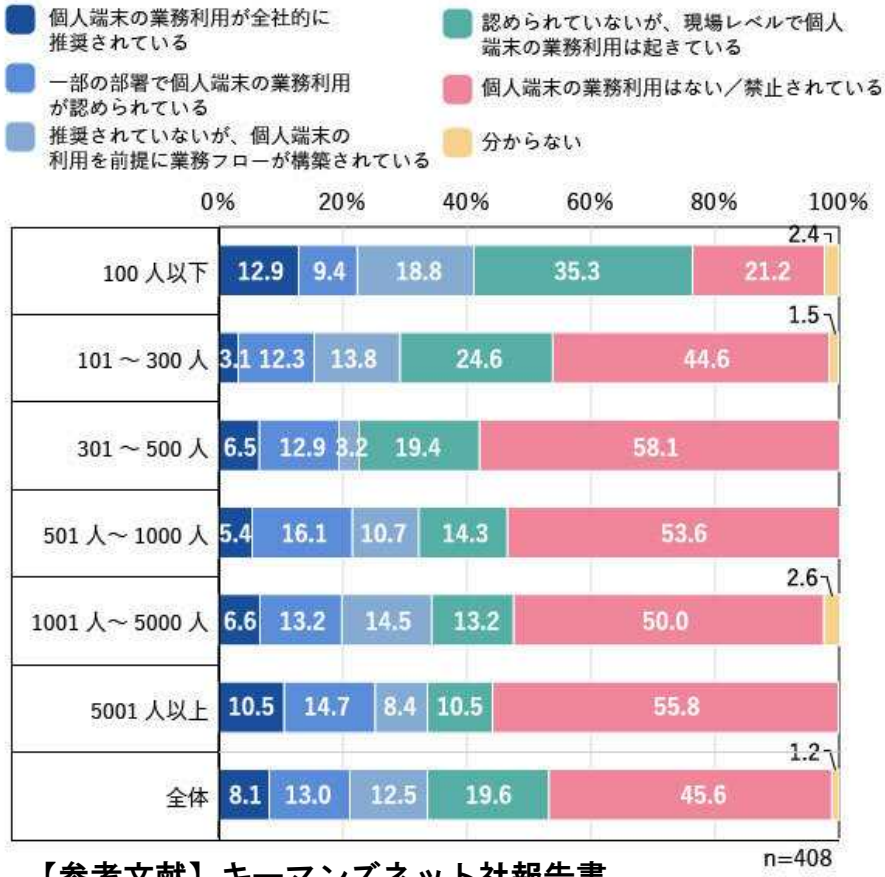


- 多くの会社が、以下の手段で接続していると思われる。
  - パソコン：VPNクライアント
  - モバイル端末：MDMもしくはTwo-factor認証
- VPNクライアントは、グローバル統一の会社だけではなく、国／会社ごとに（パソコンを手配する単位で）ソフトウェアを選定している会社もあると考えられる。
- アメリカの調査会社Report Oceanによると、多要素認証市場は、2021～2027に17%の年平均成長率を予測している。背景としては、COVID-19以降、サイバー犯罪の急増により、セキュリティを強化する会社が増えていることが考えられる。
  アジア太平洋地域でも、データ漏洩事件の増加、データ保護のための制限の実施、日本、インド、中国等でのオンライン取引増加から成長が見込まれている。

コミュニケーション環境

61. BYODの利用状況について教えてください。





- 参加会社の多く(75%)がBYODを利用。
- ただし、通信費用を会社が負担している会社は１社のみである。個人デバイスの費用負担や、MDMでどこまで管理するか、など運用面の課題も予想される。
- 日本の場合は、2020年11～12月のキーマンズネットによる調査で、全体の77.7%がBYODを禁止、非推奨だった。ただし、実態としては、全体の32.1%(12.5+19.6)は、禁止、非推奨にもかかわらずBYODを利用。

【参考文献】キーマンズネット社報告書

- 1班　システムの標準化およびデータ活用
- 2班　ベンダーマネジメント
  ・コミュニケーションツール
- **3班　働き方の変化（含むセキュリティ）**

2021年度　JUAS グローバルフォーラム　3班

テーマ

働き方の変化（含むセキュリティ）

メンバー

名前（敬称略）	Company Name
金　和寛	Konica Minolta Business Solutions Asia Pte. Ltd.
春崎　孝祐	MSIG Insurance (Singapore) Pte. Ltd.
横田　　隆	YAMAHA MOTOR ASIA PTE LTD
佐藤　綾美	IHI ASIA PACIFIC PTE.LTD.
権田　昇平	KAJIMA OVERSEAS ASIA PTE. LTD.
林　大輔	NIPPON STEEL SOUTHEAST ASIA PTE.LTD.

Jan 2022

目次

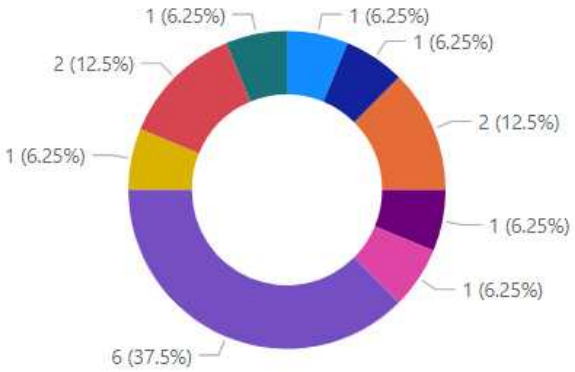
- 在宅勤務のルール、勤務管理、セキュリティ対策
- ソフトウェアライセンス管理
- フィッシング対策
- サイバー保険

アンケート回答にご協力頂き、ありがとうございました。

在宅勤務のルール、勤務管理、セキュリティ対策

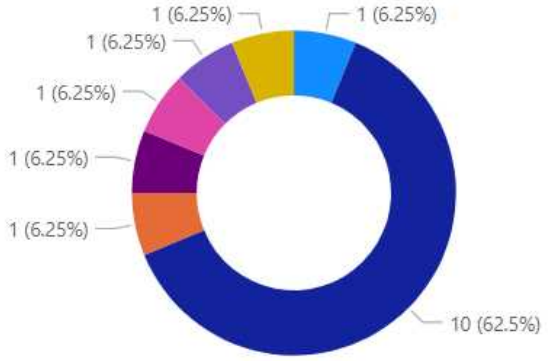
在宅勤務のルール、勤務管理、セキュリティ対策 1/5

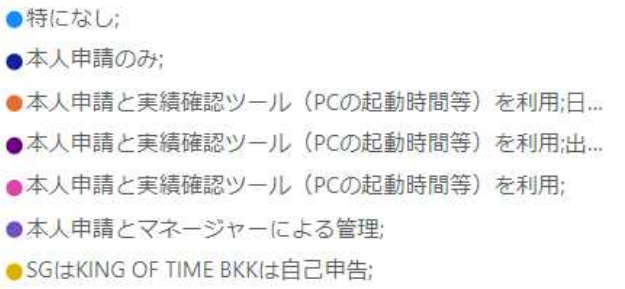
01.政府から在宅勤務、時差通勤を推奨されてますが、現在の業務時間ルールを教えてください？



フレックス9, 固定 3, シフト 4 (有効回答15、複数回答の場合あり）
日本ではコロナ感染者数も減ってることから出社数は増えています。
基本は固定だが、ITに関してはユーザーサポート時間を長めにとる為、担当によるシフト制を採用。その他の部署は固定制。
事務職はフレックス、工場はシフト;

02.日々の業務開始時間、昼休み、終了時間をどのように管理していますか？



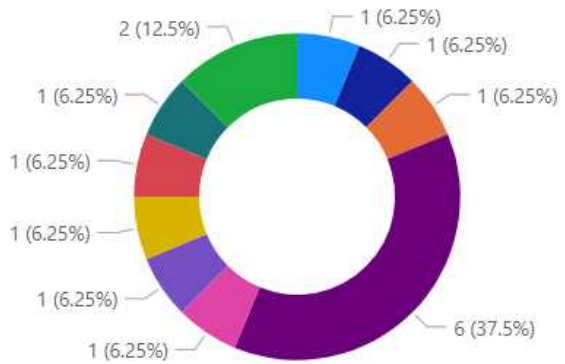


実績確認ツール 4 社は、フレックス。
日本だけですがメンバーのスマホのメール送受信時間や業務システムへのアクセス時間もみています。
出勤管理については事務所、工場への入退室管理、在宅時はスマートフォンアプリでのチェックイン、チェックアウトで管理;
SGはKING OF TIME BKKは自己申告;

在宅勤務時には、働いている状況が見えずらい
実績確認まで実施している会社は少ない。

在宅勤務のルール、勤務管理、セキュリティ対策 2/5

03.在宅勤務時に、働く場所（国）に制限はありますか？



- 自国からのみ可;出張が認められた時は隔離期間も含めて...
- 自国からのみ可;他国からも可;シンガポールではコロナの...
- 自国からのみ可;今までは海外に出ることが困難でしたの...
- 自国からのみ可;
- 原則自国からのみだが、例外あり;
- 出身国の自主隔離期間のみ他国からも可;
- 会社が承認した一時帰国中は日本からのテレワーク可;
- 他国からも可;
- ルールを検討中、または、ルールはまだない;一部の従業...

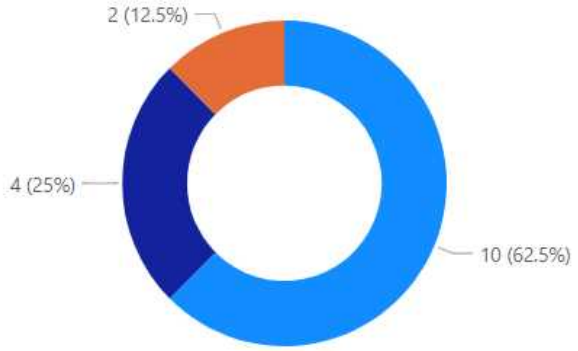
自国からのみ可 6、**一部可**　6、**他国からも可** 1, **ルール未整備**　2

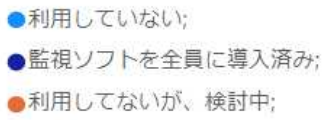
派遣者については会社が認めた一時帰国等で日本からリモートワークを行う場合あり。
会社が承認した一時帰国中は日本からのテレワーク可;
自国からのみ可;出張が認められた時は隔離期間も含めて他国から業務実施可能。但し、原則自国のみ実施。;
自国からのみ可;他国からも可;シンガポールではコロナの関係で他国からリモートワークする方もおります。;

他国から可とした場合、ＰＣ障害時の対応等、難しいと思われる

在宅勤務のルール、勤務管理、セキュリティ対策 3/5

04.PCの監視ソフトを導入していますか？





05.PCの監視ソフトを導入されている場合、製品名をご記載ください
Lanscopeが日本のみ適用されています。webroot, cybereasonがウイルス対策ソフトとして入っています。
Symantec Endpoint Protection スマートフォンの出勤管理アプリは自社開発
Windows Defender
グループ会社作成のツールを利用中。 業務分析、情報漏洩対策のため、Controlioへの変更を検討中。

監視ソフトという意味では、1社のみ導入済み。

Monitoring software	Email response time	Log on/off times	Time on social media	Keyboard/mouse activity	Webcam	Email content	Keyword alerts	Employee might be unaware
ActivTrak		√	√	√				√
TimeCamp		√	√	√				
InterGuard	√	√	√	√		√	√	√
Hubstaff			√	√				
Teramind		√	√	√		√	√	√

https://www.newsweekjapan.jp/stories/world/2021/11/post-97498.php
https://www.washingtonpost.com/technology/2021/08/20/work-from-home-computer-monitoring/

在宅勤務のルール、勤務管理、セキュリティ対策 4/5

06.PCからの情報漏洩対策は、どのように実施されていますか？
特に目立った情報漏洩対策は実施しておらず、一般的なアカウントへの権限付与・棚卸により管理しているのみ
情報漏洩対策ツールを導入している。
外部デバイスの利用制限、 アプリ利用ログ、 Webアクセスログ
ハードディスク暗号化による盗難時の対策のみ実施
セキュリティ対策のソフト導入、データ保存や持ち出しに関するルール制定などしているが、悪意をもって情報をリークする行為へのリスクなどに対して罰則等以外は対応しきれていない。
この観点からは特にしていない。
クラウド環境（BOX利用）を推奨
エンドポイントセキュリティツールのインストール
いろいろ
アンチウイルスソフトのファイヤーウォール機能でポートを制限。
USBやBluetooth接続をブロック
USBメディアのブロック、ファイル共有サイト・外部メールのブロック、ソーシャルメディア等のアクセス監視。
USBブロック（日本）、メールは２年間オンラインアーカイブ取得（全グループ）、CASBにてWEBサイトへの情報アップロードの監視（全グループ）、URLフィルタ（Gmail利用不可など（日本のみ））を実施
IBM-SOCによるフィルタリングとネットアクセス監視、入力制限（クレジットカード番号等）を実施
DLP導入とUSBメモリー利用不可
・ガイドライン（重要データはローカル保存禁止） ・PC/ネットワーク監視（FireEyeHX,NX）

＜キーワード＞

USB（外部デバイス）制御：５
ログ・監視：４
ルール、罰則：２
URL**フィルター**：２
エンドポイントセキュリティツール：２
ファイル共有ツール：１
HDD**暗号化：１**

＜先進的な取り組み＞

情報漏洩対策ツール（DLP）：２
CASB（CloudAccess Security Broker：**キャスビー**）**の利用：１**
SOC**サービス：１**

在宅勤務のルール、勤務管理、セキュリティ対策 5/5

07.在宅管理のルール、業務管理、セキュリティ等に課題があれば、教えてください。
CSABやSASEの導入の検討。
PCのセキュリティ・監視は強化し、抑止力に期待している。 一方、自分のスマホ等ではできるため、完全にはブロックできない。
Web会議が隙間なく入れられる。何か会社でルールはありますか？会議と会議の間は15分あける、会議は最長45分等。
在宅ルール：弊社シンガポールオフィスでは、コロナ規制あけ次第、原則出社することが会社方針となっています。（在宅勤務時は申請が必要）
セキュリティ：SNSツールなどによるデータ漏洩リスク
在宅勤務を拡大したが、従来のセキュリティ対策のままであること コロナにより電子化・システム化が推進され、容易に情報を持ち出せる環境になっており情報漏洩などの対策が必要
業務の実績管理の仕組みがないこと
業務管理にITを活用して効率を上げたいが、自社にFitするものが見つかっていない。
社員は在宅勤務時はパソコンを持ち帰っているが紛失や盗難のリスクがあるが、VDI導入など全面的に進めるにはコスト面などで課題があります。
管理職のメンバーのマネジメントにおいては決まった方法等がないので、コロナが続くようであれば、リモートワークにおけるチームビルディングやマネジメントスキルも必要になってくるかと思います。
自宅以外からの業務は禁止としている。

情報漏洩・セキュリティ 5
在宅・会議ルール 3
業務管理・チームビルディング 3

【前頁にあった下記の取り組みのご紹介】
情報漏洩対策ツール（DLP）
CASB（CloudAccess Security Broker：**キャスビー**）**の利用**

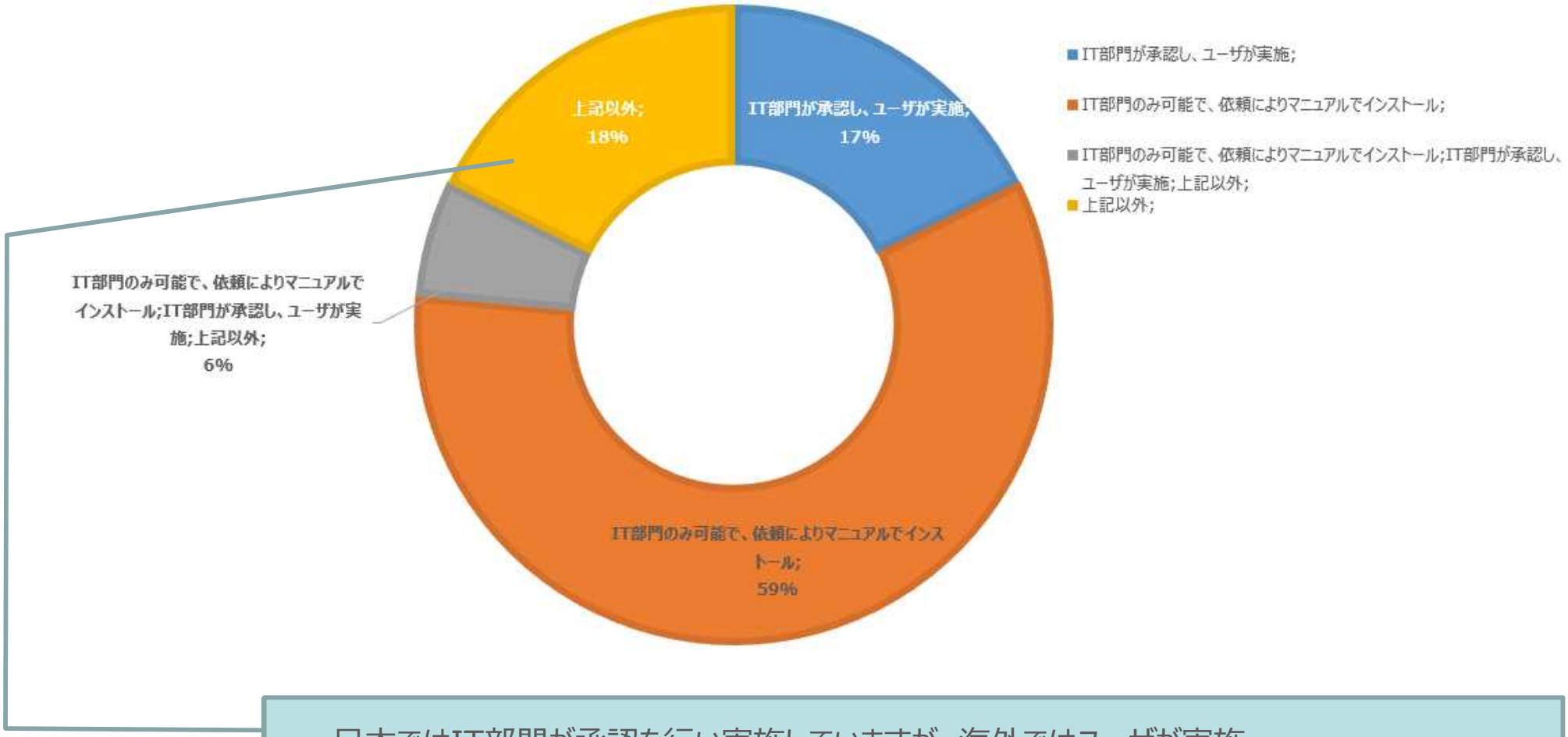
在宅勤務を続けるのでばれば、そのルール、
パフォーマンスが上がる取り組み等を将来、議論してみたい。

JUAS

ソフトウェアライセンス管理

ソフトウェアライセンス管理（1/4）

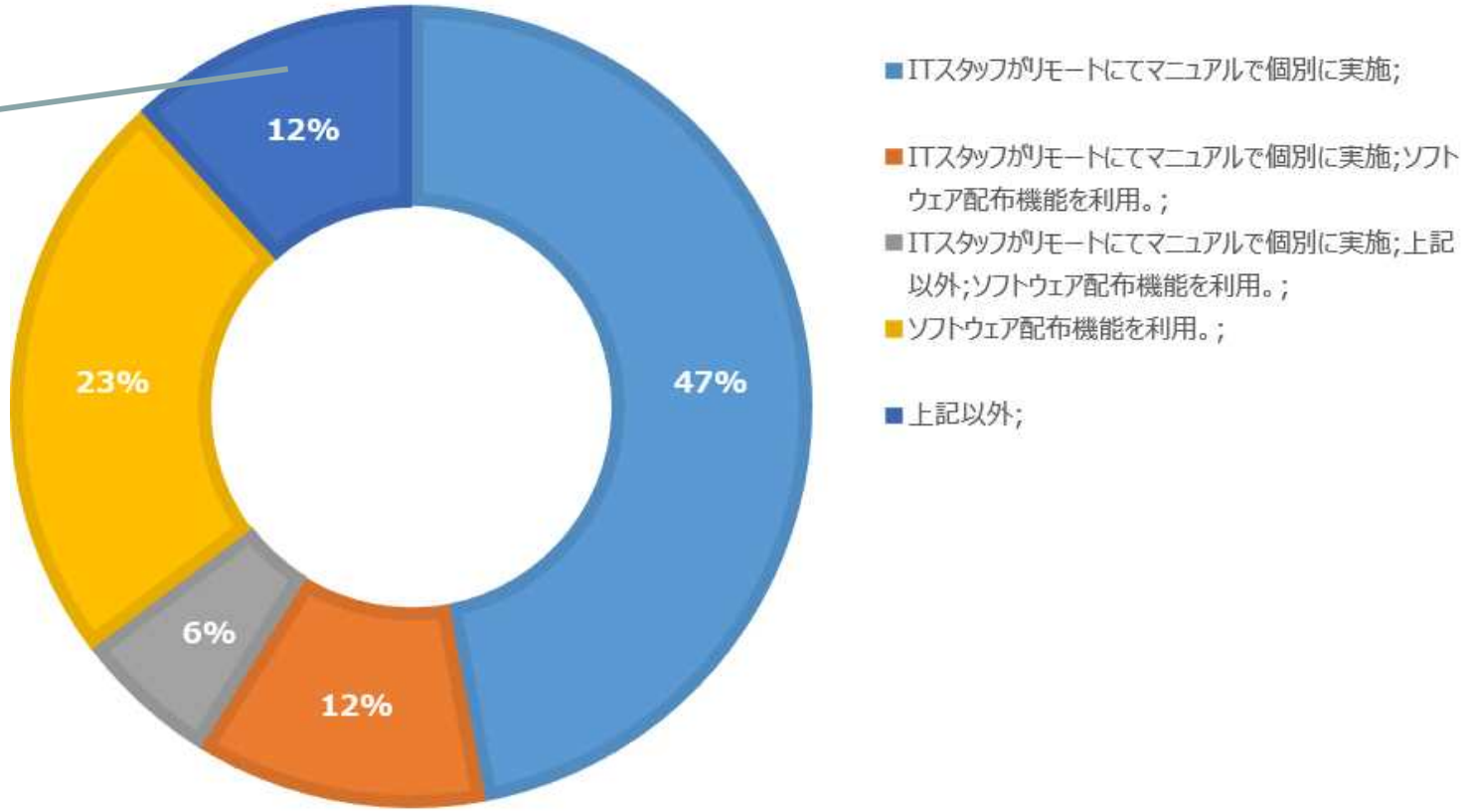
PCへのソフトウェアのインストールは、どのように実施していますか？



- 日本ではIT部門が承認を行い実施していますが、海外ではユーザが実施。
- 駐在員を除きIT部門のみ可能。
- IT部門でエンドポイント管理ツール（Tanium）を利用してインストール。

ソフトウェアライセンス管理（2/4）

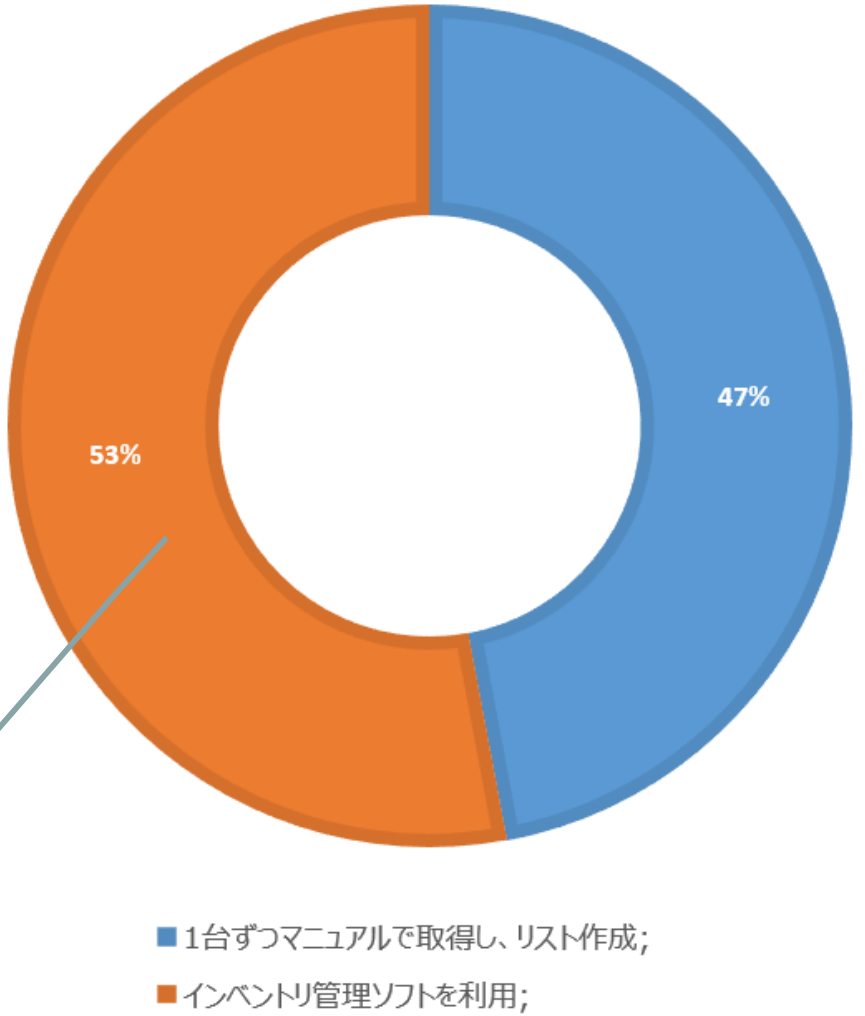
在宅勤務時に各PCへのエージェントファイル等のプログラム一括インストールは、どのように実施していますか？



- 駐在員を除きITがリモートにてマニュアルで個別に実施。
- エンドポイント管理ツール（Tanium）の配布機能を利用。
- 特別に出社して対応することもあります。
- ITスタッフが各PCを回収してインストールし、利用者に返却する。

ソフトウェアライセンス管理（3/4）

ソフトウェアインベントリ取得・管理方法を教えてください



- PC management tool
- Bigfix
- Lanscope
- Tanium
- Manage Engine
- Symantec Endpoint Protection
- ISM CloudOne（3社）

ソフトウェアライセンス管理（4/4）

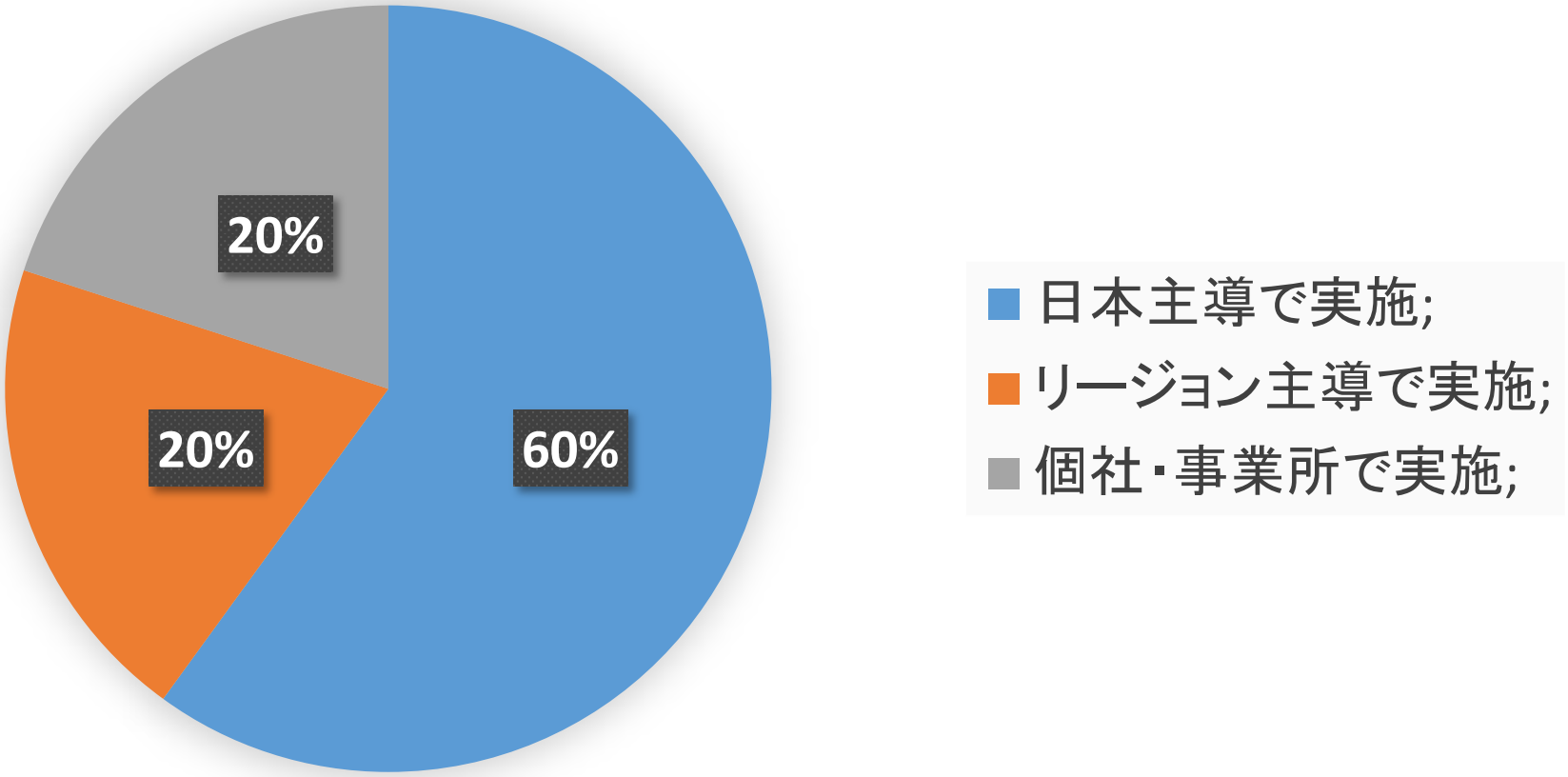
ライセンス管理、インストール運用、インベントリ管理に課題があれば教えてください。

マイクロソフトのライセンスはグローバル調達できておらず、各販売代理店からのリストの提供もフォーマットがバラバラなので整理に時間を要しています。
一括ソフトウェアのインストール、取得できないexeファイルのソフトウェア、複雑なライセンス形態とインベントリのチェック
マニュアル管理からソフト管理への移行。
ライセンス管理の自動化は始めたばかり。
皆さんがなんのソフトを使っているのか知りたいです
在宅勤務になり、ソフトウェアのアップデートに時間を要するようになってしまった。

フィッシング対策

フィッシング対策

メールのフィルタリングはどのように実施していますか？



フィッシング対策

ユーザからIT部門への不審メール報告・問い合わせ頻度はどの程度ですか？

不審メール報告・問い合わせ頻度は、コロナ前後で変化がありましたか？

フィッシング対策

【自社の取り組み紹介や、他社に聞きたいことがあれば記述ねがいます（例：外部からのメールにはメール先頭にExternalを付ける等。）】

社外メール受信時の対応

- 社外メール送信時、毎回、送信可否を訊ねるポップアップが起動します（ユーザからは不評）
- 社外メール受信時、ポップアップで注意喚起され、また、社外ドメインであることを示すワッペンがメール先頭に埋め込まれます。件名にも”#####”が自動付与されます。
- フリーメールアドレスからのメール先頭にFREE MAILを付けている
- 外部からのメールにはヘッダー部分に注意喚起文をつけています。

その他

- メールソフトにaddonしたPhish me tool で不審メールを報告できます。
- 今のところフィルタリング・年1回のフィッシングメール訓練のみです。

フィッシング対策

【自社の取り組み紹介や、他社に聞きたいことがあれば記述ねがいます（例：外部からのメールにはメール先頭にExternalを付ける等。）】

意見交換

- URLフィルタはどこまで厳密に管理されていますか？（ユーザ単位、グループ単位、全社同じ？など）
- メール対策をどのぐらい実施しているのか（SPF、DKIM、DMARC）
- PPAPを禁止しているか、ファイル共有サービスなどの利用有無
- クラウドシステムから自社ドメインでメール送信したいなどの要望にどうやって対応しているか"

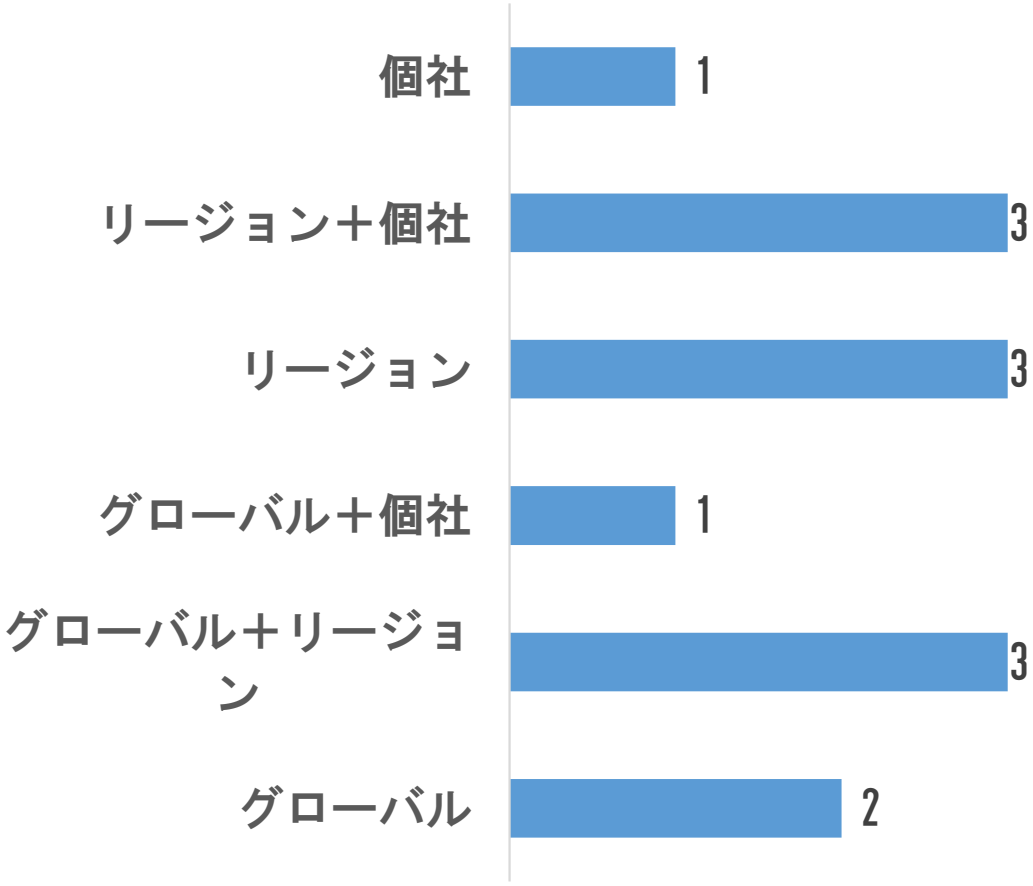
フィッシング対策

ユーザへのセキュリティ教育（フィッシング詐欺に関して）の実施有無をご回答ください？

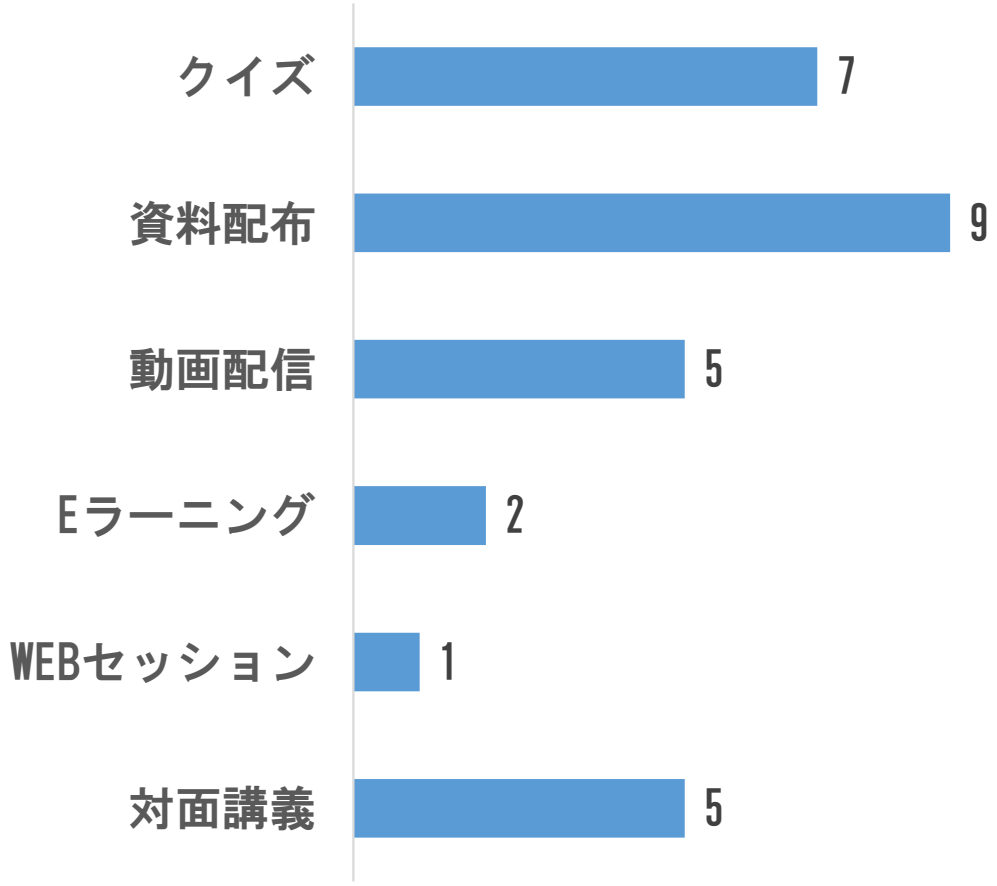
ユーザへのセキュリティ教育を定期的に実施している場合、頻度はどの程度ですか？

フィッシング対策

ユーザへのセキュリティ教育の教材はどこで作成していますか？（複数回答可）

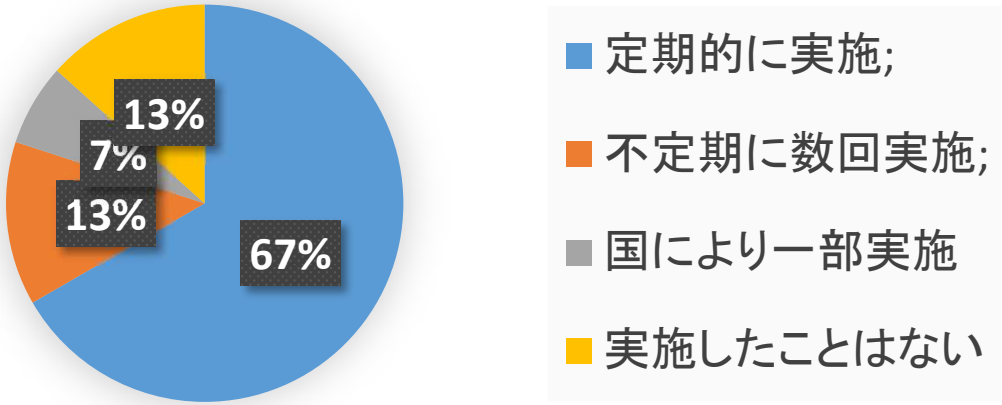


ユーザへのセキュリティ教育の内容、形式（複数回答可）をご回答ください

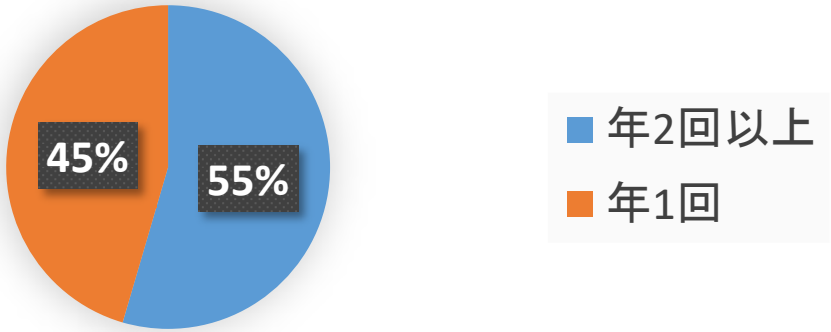


フィッシング対策

標的型攻撃メール訓練の実施有無をご回答ください



標的型攻撃メール訓練を定期的に実施している場合、頻度はどの程度ですか？



【標的型攻撃メール訓練のKPIをご記載ください】
- 部門ごとのクリック件数、率、報告率等。
- クリック率10%以下、報告率50%以上等の具体的な目標値を決めている企業もあった。

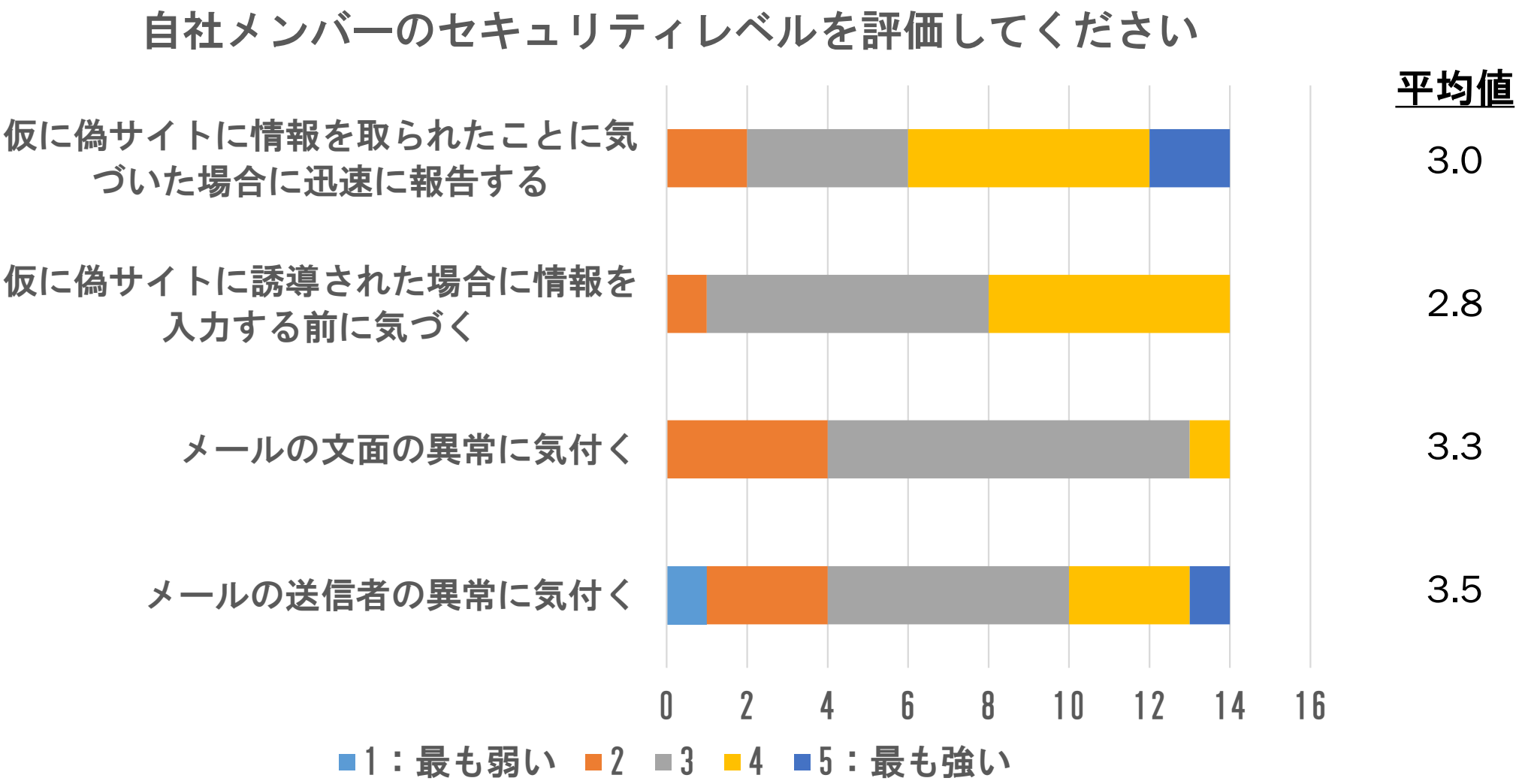
フィッシング対策

【自社の取り組み紹介や他社に聞きたいこと】
・本社から、例えば、Emotetが流行っているから気を付けるよう連絡はある。だだし、IT部門以外が理解するのは、難しいかもしれない。

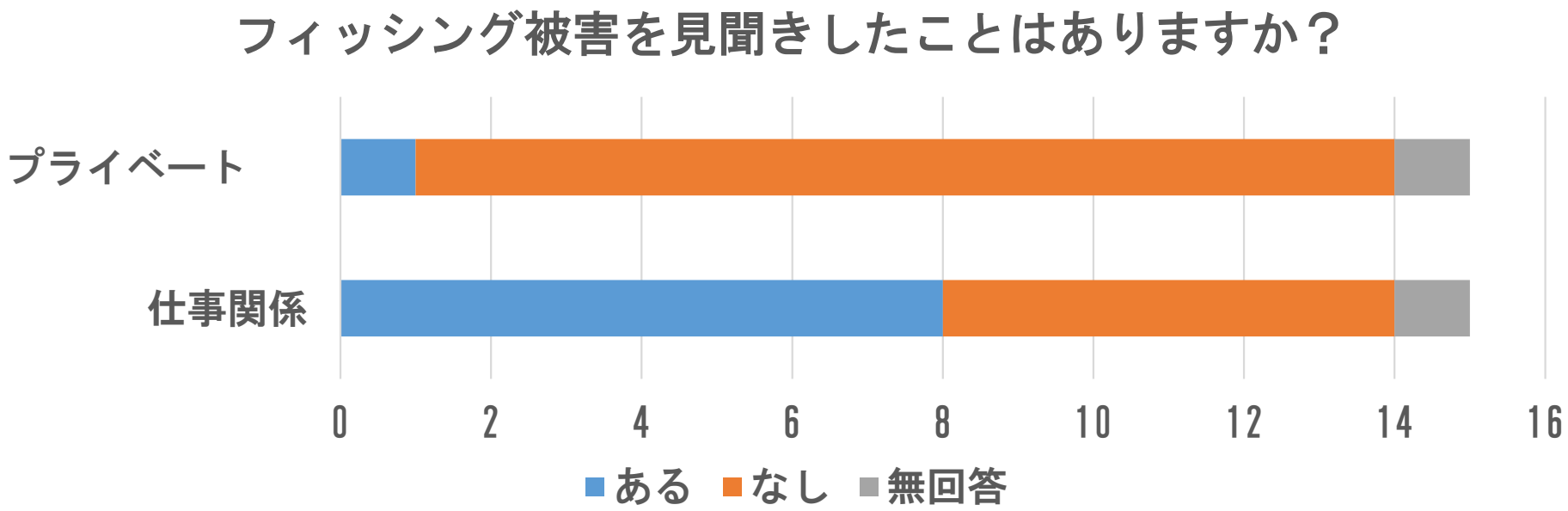
・Office365のAttack Simulatorを使われているなら、どのように使っているのか、使いやすいかなど聞いてみたい

・シンガポール国内ではKnowBe4を利用して、情報セキュリティ教育を実施。フィッシングメール訓練、情報セキュリティ講習資料（動画、クイズあり）も充実して便利です。

フィッシング対策


自社メンバーのセキュリティレベルを評価してください
平均値
仮に偽サイトに情報を取られたことに気づいた場合に迅速に報告する
3.0
仮に偽サイトに誘導された場合に情報を入力する前に気づく
2.8
メールの文面の異常に気付く
3.3
メールの送信者の異常に気付く
3.5
0
2
4
6
8
10
12
14
16
1：最も弱い
2
3
4
5：最も強い

フィッシング対策



- 半年に一度くらいの頻度で、口座情報変更の詐欺被害（未遂含め）が発生しています。都度、システム・運用での被害防止策検討をしていますが、どこまでやってもいたちごっこだし、マニュアル判断が入る以上、被害をゼロにできないという印象です。

- ハッカーからのフィッシングメールが送られ、IDとパスワードを入力するよう促され、実際に入力してしまった社員がいた。その後、そのIDを使ってフィッシングメールが拡散された。

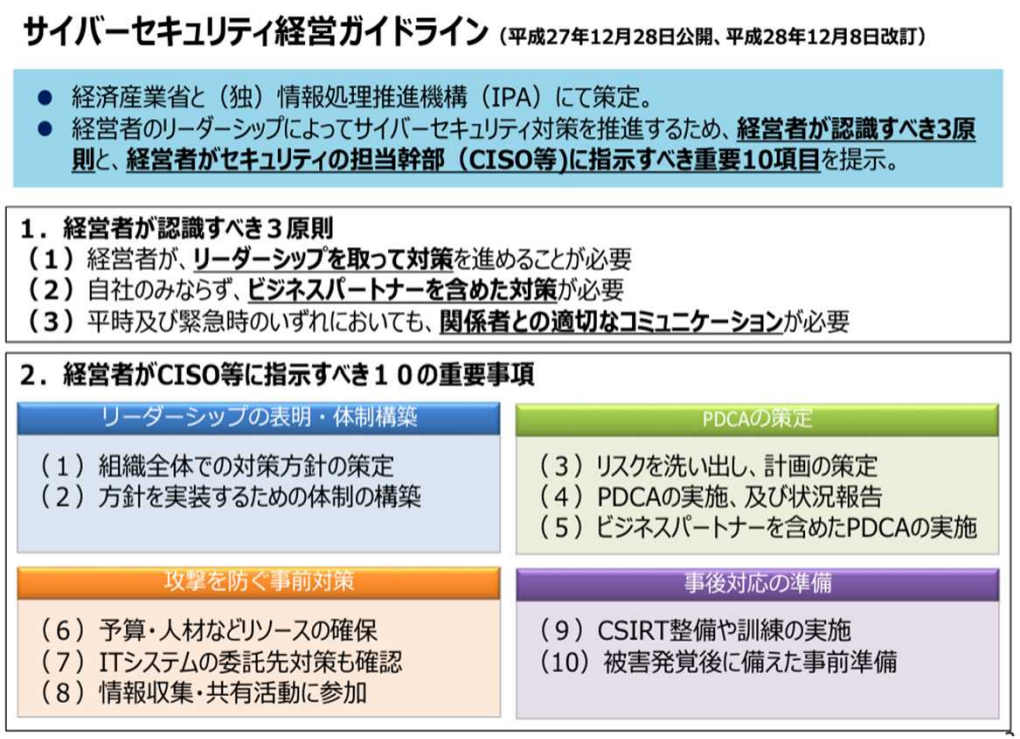
フィッシング対策

- 取引先を騙ったメールで銀行支払の連絡があり、支払をした。
- 送信者は、実際の取引先会社名、担当者名が使われていた。
- 海外販社でフィッシング被害にあい、メールのID・PWが流出しメールを乗っ取られた（なぜかそのユーザだけ多要素の設定が出来ていなかった）。取引先含め千数社へメールがばらまかれたが、幸い情報漏洩はそのユーザのID・PWに留まり大事にはなりませんでした。
- すぐにIDを停止の措置を取ったため間もなく復旧したが、外部の専門家によるフォレンジックや弁護士も入れた対応などを実施したため、結構な費用が発生したと聞いています。
- 友人がLineの乗っ取りにあい、急に私にコンビニでRakutenカードを買うように言われましてその会話で遊んだ事はあります。本人には伝えていたので途中でアカウントが締結されたため会話は終了しました。"

サイバー保険

サイバー保険について – サイバーセキュリティ経営ガイドライン

経済産業省から公表されている「サイバーセキュリティ経営ガイドライン」では、「サイバーセキュリティは経営問題」としたうえで、セキュリティ対策の実施は「コスト」ではなく、将来の事業活動や成長に必須な「投資」ととらえることが重要であるとし、「セキュリティ投資は必要不可欠かつ経営者としての責務である」と対応を求めています。
同ガイドラインには、経営者がサイバーセキュリティ対策を実施するうえで指示すべき「サイバーセキュリティ経営の重要１０項目」が以下のとおり纏められており、そのうち「サイバーセキュリティリスクの把握とリスク対応に関する計画の策定」の項目において、把握したリスクに対する対策（リスク移転策の実施）の一つとして、サイバー保険の加入があげられています。



出典：経済産業省HP　サイバーセキュリティ経営ガイドラインの改訂ポイント
https://www.meti.go.jp/policy/netsecurity/downloadfiles/overview.pdf

指示４　サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

経営戦略の観点から守るべき情報を特定させた上で、サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、リスクに対応するための計画を策定させる。その際、サイバー保険の活用や守るべき情報について専門ベンダへの委託を含めたリスク移転策も検討した上で、残留リスクを識別させる。

対策を怠った場合のシナリオ

- 企業の経営戦略に基づき、各企業の状況に応じた適切なリスク対応を実施しなければ、過度な対策により通常の業務遂行に支障をきたすなどの不都合が生じる恐れがある。
- 受容できないリスクが残る場合、想定外の損失を被る恐れがある。

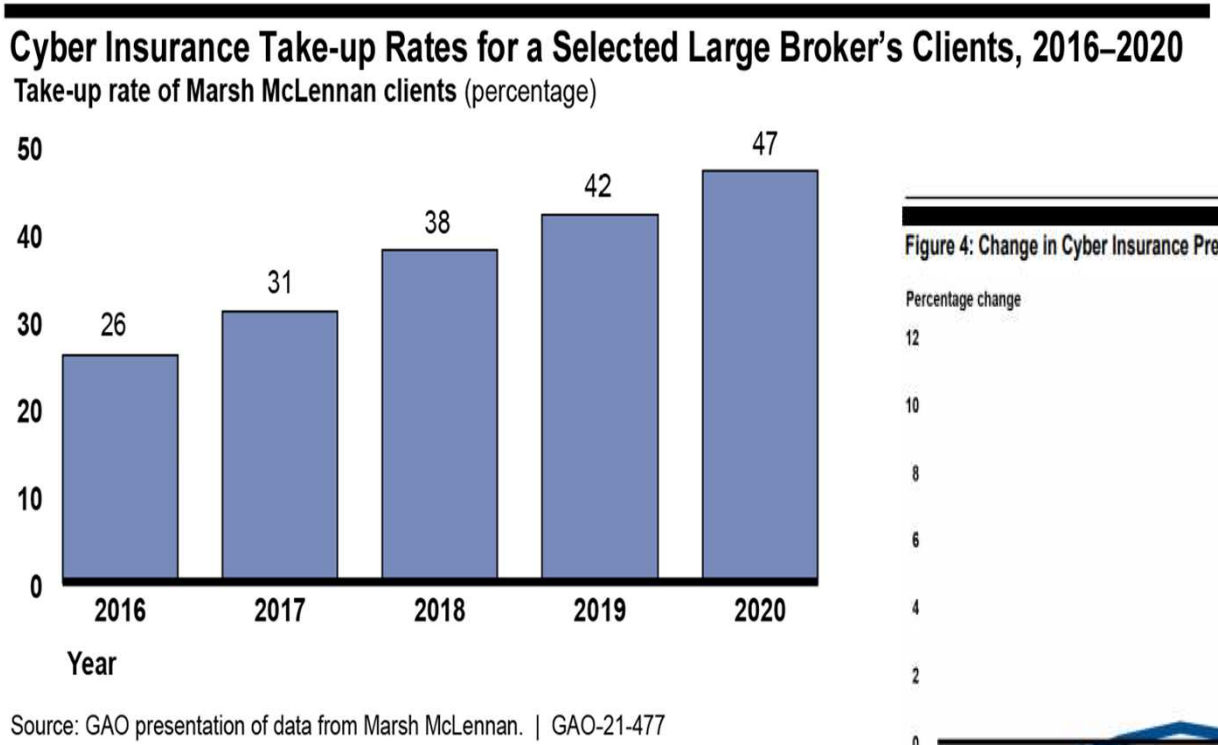
対策例

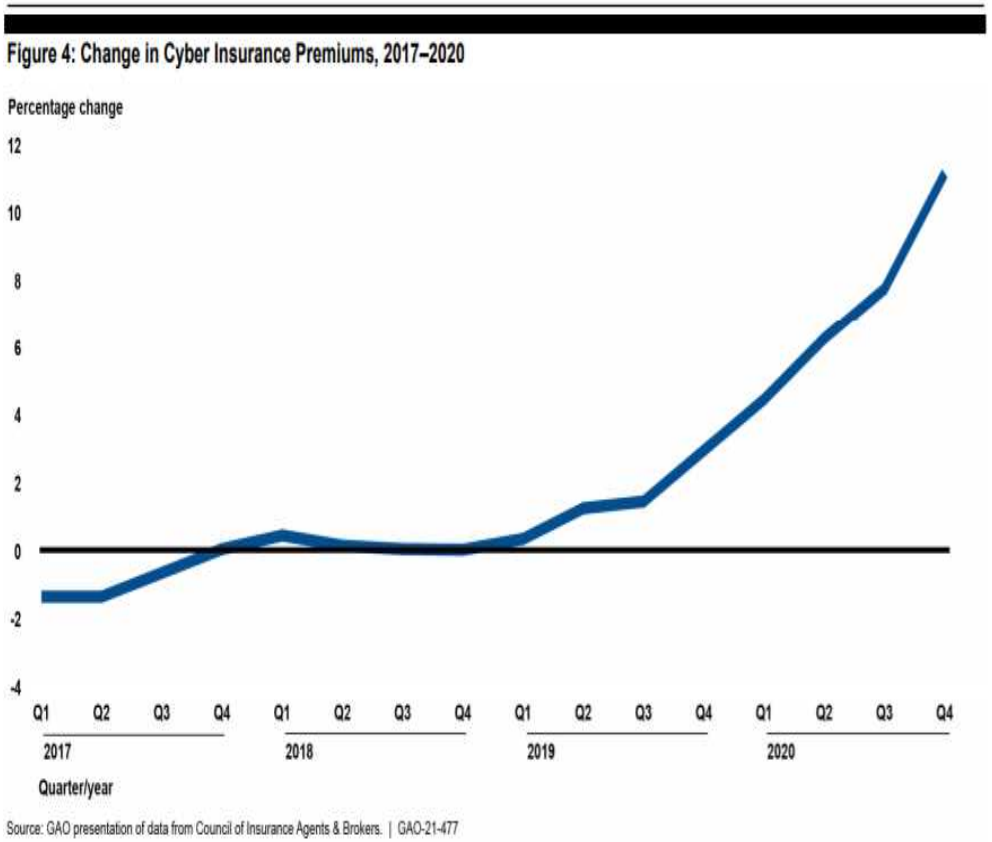
- 組織における情報のうち、経営戦略の観点から守るべき情報を特定し、それらがどこに保存されているかを把握する。
- 守るべき情報に対して、発生しうるサイバーセキュリティリスク（例えば、経営戦略上重要な営業秘密の流出による損害）を把握する。
- 把握したリスクに対して、実施するサイバーセキュリティ対策を以下の観点で検討する。
  - ✓ リスク低減策の実施（リスクの発生確率を下げる対策）
    例：重要な情報へのアクセス制御、ソフトウェア更新の徹底
  - ✓ リスク回避策の実施（リスクが発生する可能性を除去する対策）
    例：端末の持ち出し禁止（外部での盗難のリスクを回避）
  - ✓ リスク移転策の実施（リスクを他社等に移す対策）
    例：クラウドサービスの利用、**サイバー保険の加入**
- リスクの発生確率や、発生したときの損害等を考慮して、サイバーセキュリティ対策の実施が不要と判断したリスクについては残留リスクとして識別する。
- 法令上、安全管理措置が義務づけられている情報については、法令上の取り扱いも考慮したリスクの特定と緊急時に速やかに情報の保護が行えるような対策となっているかも検討する。
- 製品・サービス等においてセキュリティバイデザインの観点を踏まえて企画・設計段階からサイバーセキュリティ対策を考慮する。

サイバーセキュリティ経営ガイドライン Ver2.0
http://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf

サイバー保険について　– サイバー保険の動向

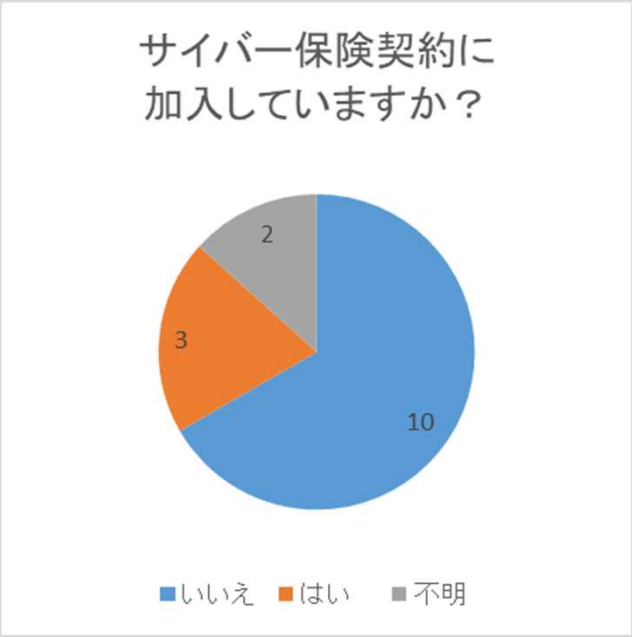
米国会計検査院（GAO）のレポートによると、サイバー攻撃が頻発するようになった結果、サイバー保険の加入率は増加傾向にあるが、保険料が高騰しており、また補償額の上限を減らしたり、特定の補償に限定している。2021年もその傾向が続く可能性が高いとのこと。





出典：U.S. Government Accountability Office HP
https://www.gao.gov/assets/gao-21-477.pdf

サイバー保険について　－　アンケート結果



保険加入されている場合

① 契約の主体者：本社
② 保険の補償範囲：費用損害（他は不明）／賠償損害と費用損害
③ 付随サービスの内容：外部セキュリティ評価（セキュリティ脆弱性）
④ 加入に至った経緯
- ✓ 昨今増えてきているサイバー攻撃に対するリスク管理の一環
- ✓ 昨今のサイバー被害拡大を受けて本社主導で加入。

保険加入されていない理由

- ✓ まだ加入していないが、近い将来加入予定。
- ✓ 検討したが、現時点で加入予定はない（情報は常に収集中）
- ✓ 内容がよくわからないため
- ✓ 本社も利用してなく、必要なのかを判断できてない。
- ✓ 加入する絶対的な理由がまだなく、本社側でも加入していないため。
- ✓ 弊社としては、保険よりも、未然に防止する仕組みの整備に、お金を使っている
- ✓ 何かがあったときには、自社内で確認・調査できる体制（+予算）を整えている
- ✓ 補償内容が見合わないため
- ✓ 高価。
- ✓ 保険料に比して求償範囲が狭く割に合わないため。
- ✓ コストメリットについて経営層に明確に提示できていないため

End of Document