2020年度　ITインフラ研究会
分科会A　活動報告資料

研究チーム

- コロナ禍で求められるITインフラ
- 適正ITコストの見極め方
- 海外・グループ会社ガバナンス

2021年4月

ITインフラ研究会　分科会A

概要（選定テーマ）

分科会Aは、「インフラ領域の企画・統制研究」を実施していくことを目的として、11名のメンバーが以下のような関心事項を元にテーマ選定を実施。

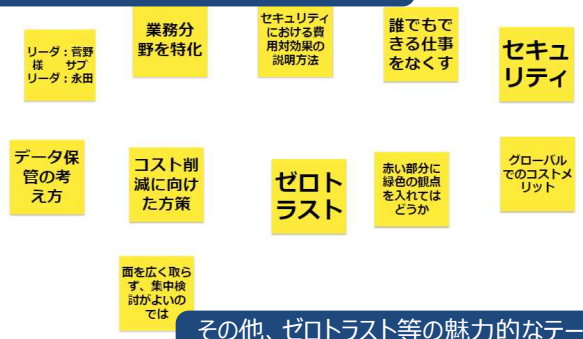
No	回答分野
1	クラウドシフト／インフラの在り方
2	開発におけるインフラの在り方・提案
3	チーム運営
4	社内基準策定に向けた視点・視座
5	統制の効かせ方／ニーズへの応え方
6	グローバルNW・セキュリティ
7	ロードマップ策定
8	IT基盤統一化・標準化
9	endpoint/sd-wan/SWG/Aaure
10	テレワーク／在宅環境あるべき姿
11	企業ネットワークの将来像
12	企画・統制に関するノウハウ
13	重点事業・削減・効率化インフラ企画
14	長期目線の事業戦略の組み立て方

研究テーマ
1．コロナ禍で求められるITインフラ
2．適正ITコストの見極め方
3．海外・グループ会社ガバナンス

テーマ選定の様子

まさにコロナ禍ということで、今年は原則すべてリモートで行った。
Jamboardを駆使し、以下のように活発に議論が進み、それぞれのテーマ選定に至る。

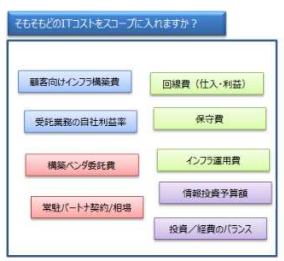
第一回分科会(全体ブレスト)



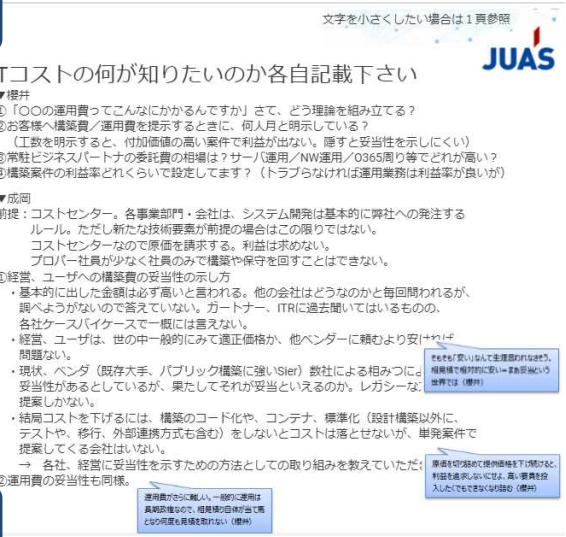
【主なキーワード】
- **コスト**
- **セキュリティ**
- **コロナ禍のIT**

その他、ゼロトラスト等の魅力的なテーマもあったが、他チームテーマということで、残念ながら見送り。

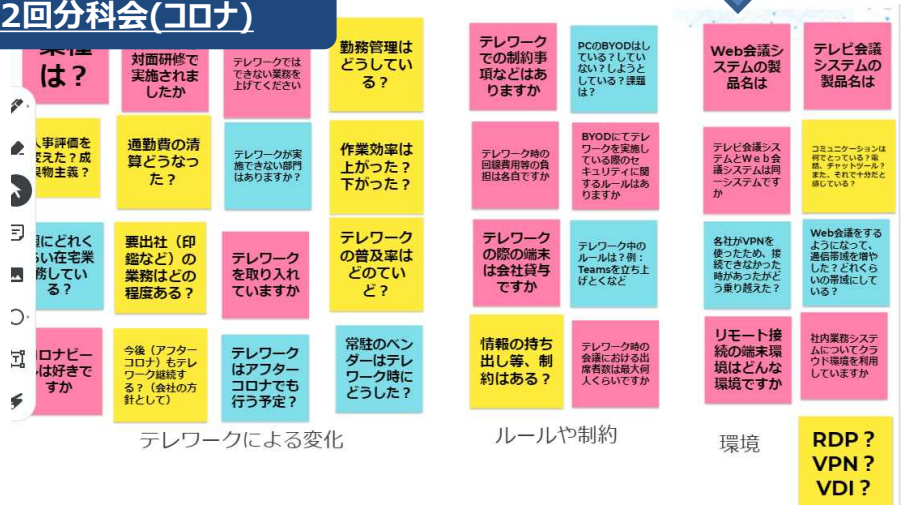
第2回分科会(適正ITコスト)



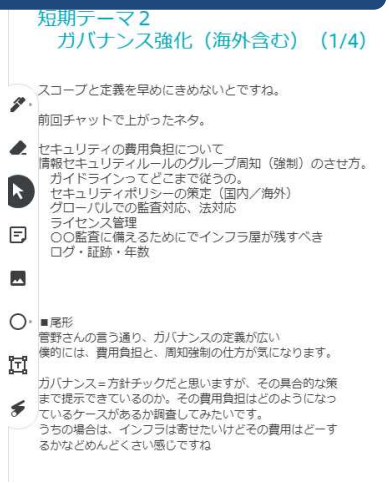
自社のコスト（原価）？
お客様目線でのコスト？
で、どこの科目？
の何のトレンドを知りたい？

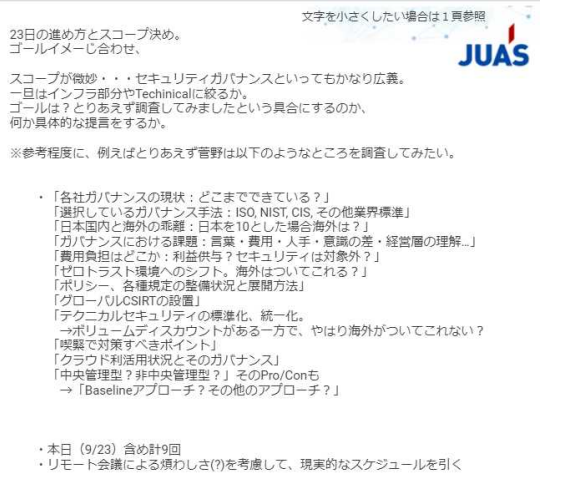


第2回分科会(コロナ)



第2回分科会(ガバナンス)





メンバー紹介（ユーザー多め、いい塩梅でチーム分け）

テーマ１ コロナ禍で求められるITインフラ	テーマ２ 適正ITコストの見極め方	テーマ３ 海外・グループ会社ガバナンス
Theme-Leader 山田 ユーザー（電力）	Theme-Leader 成岡 ユーザー（リース）	Leader 菅野 ユーザー（建設）
Sub-Leader 永田 情報子会社（保険）	Sub-Leader 櫻井 ユーザー（食品）	尾形 情報子会社（電力）
芦川 ユーザー（製造）	大久保 ソフトウェア・パッケージ販売 サポート	川崎 ユーザー（医薬品）
石本 SIer（独立系）	尾崎 ユーザー（電力）	

連携　連携

年間スケジュール（概ね月次開催/全てZoom会議）

■ 前項で設定したテーマに基づき、
以下のようなスケジュールで打ち合わせ、研究を行った。

会議体	日時	実施内容
第1回全体会	8/5 (水)16:00～	顔合わせ、活動方針説明/グループ分け、研究テーマ検討
第1回分科会	8/26(水)15:00～18:00	具体的な課題設定と、得たい結論（成果）イメージ合わせ
第2回分科会+全体会	9/23(水)14:00～16:00	定例会での進捗報告　各リーダからから、方向性の共有
第3回分科会	10/14(水)15:00～18:00	分かれたテーマ毎に進め方のイメージの共有
第4回分科会+全体会	10/30(金)14:00～16:00	テーマ毎でのディスカッション定例会での進捗報告
第5回分科会	11/18(水)15:00～18:00	テーマ毎でのディスカッション
第6回分科会+全体会	11/27(金)14:00～16:00	テーマ毎でのディスカッション定例会での進捗報告
第7回分科会	12/16(水)15:00～18:00	テーマ毎でのディスカッション
第8回分科会+全体会	1/27(水) 14:00～16:00	テーマ毎でのディスカッション定例会での進捗報告
第9回分科会	2/17(水) 15:00～18:00	最終成果物の仕上げ（当初の課題は解決できていそう？）
第10回分科会+全体会	3/3 (水)　14:30～18:00	定例会での最終成果物報告発表

研究テーマ

◆次項より、以下のテーマごと研究内容

1. コロナ禍で求められるITインフラ
2. 適正ITコストの見極め方
3. 海外・グループ会社ガバナンス

2020年度ITインフラ研究会

分科会A　活動報告
-コロナ禍で求められるITインフラ

世間の印象 と 現場のGap, 埋めませんか…？

ITインフラ研究会　分科会A
コロナ禍で求められるITインフラチーム

アジェンダ

1.コロナ禍における各社での状況

2.テレワークよる業務等の変化

3.テレワークにおけるルール等

4.各社での業務インフラ環境

5.まとめ

アジェンダ

1.コロナ禍における各社での状況

2.テレワークよる業務等の変化

3.テレワークにおけるルール等

4.各社での業務インフラ環境

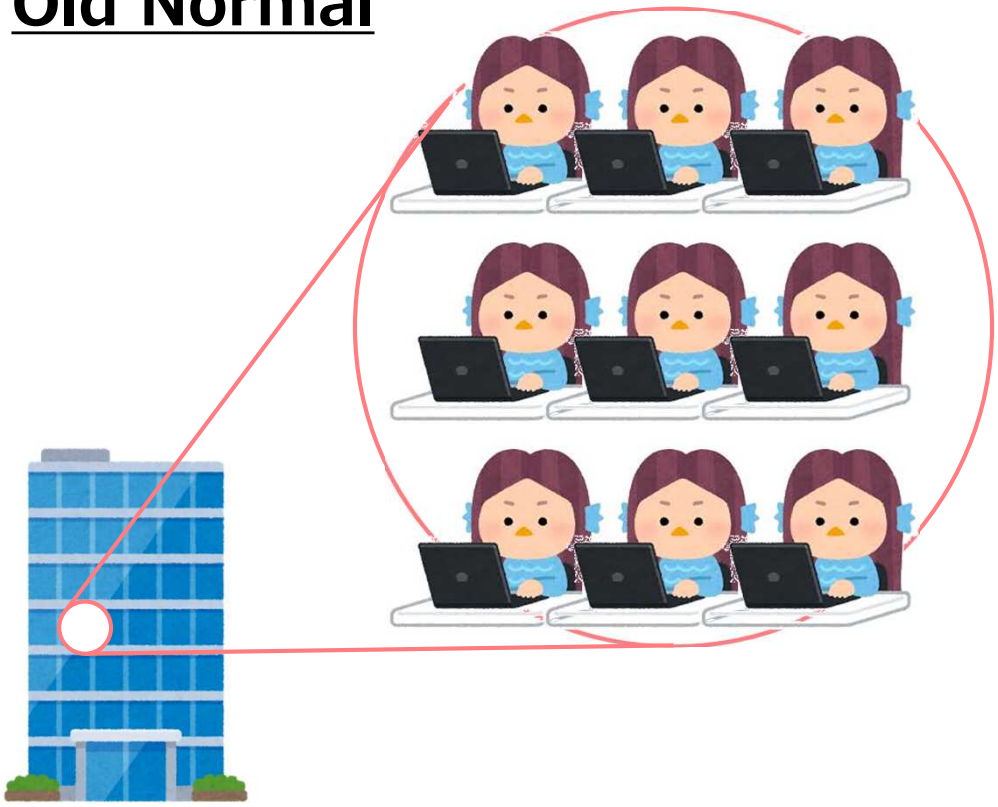
5.まとめ

1.コロナ禍における各社での状況

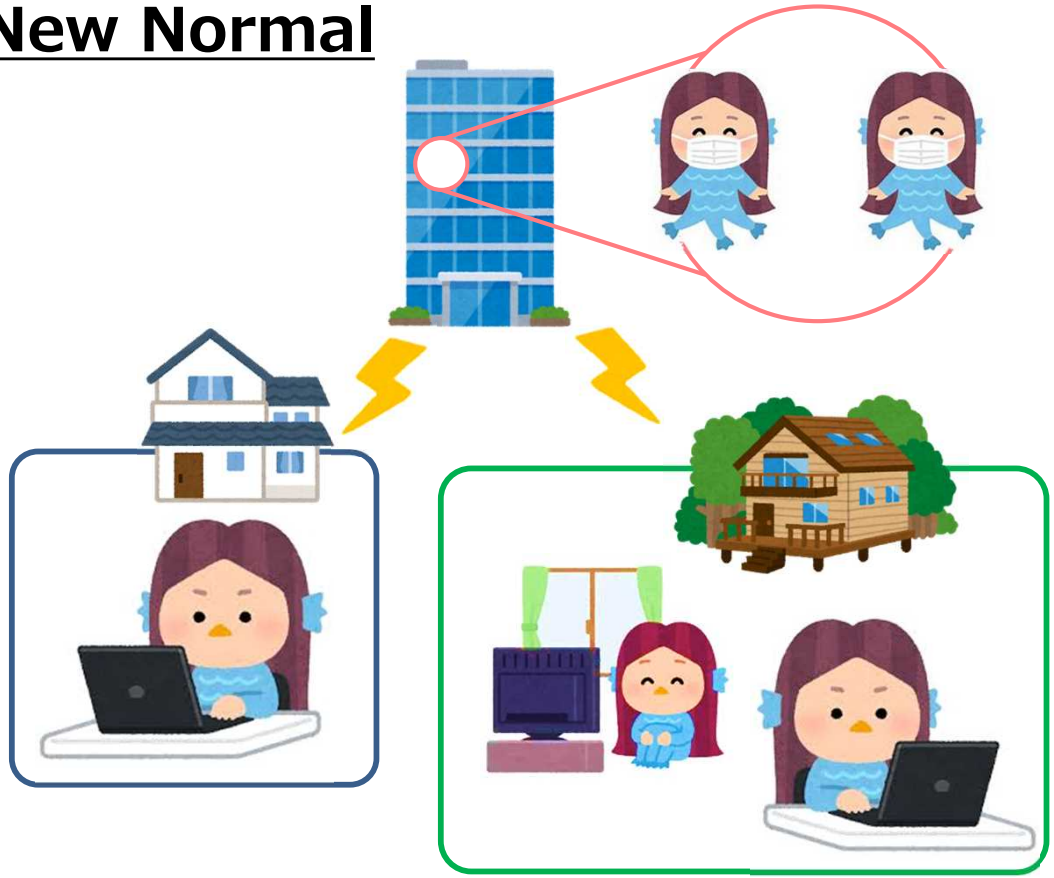
新型コロナに伴う変化

- ✓ 新型コロナウイルスの登場により，従来の標準が崩壊し，変化への対応が強いられた
- ✓ ビジネス社会においては，『仕事のオンライン化』『居住地と職場の分離』など，新しい働き方が進み，個々人にあった働き方が必要となっている

Old Normal

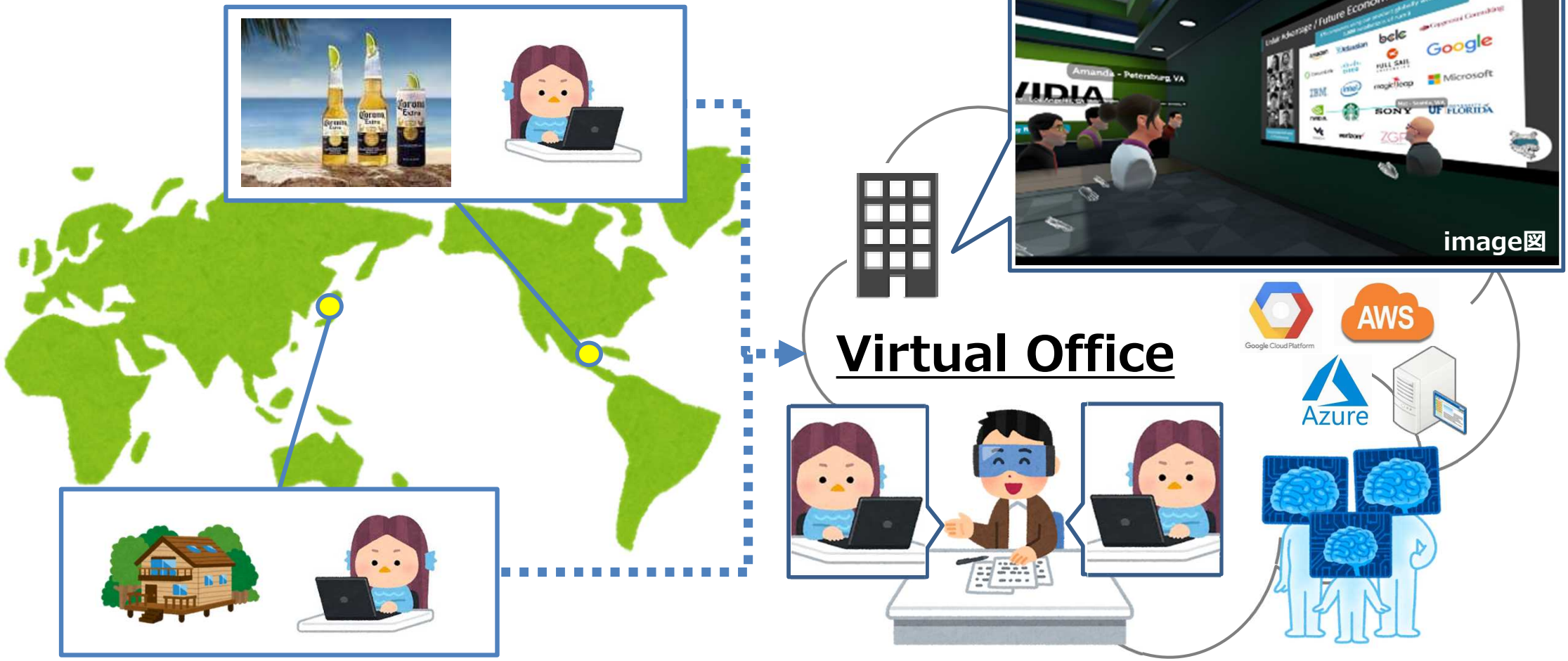


New Normal



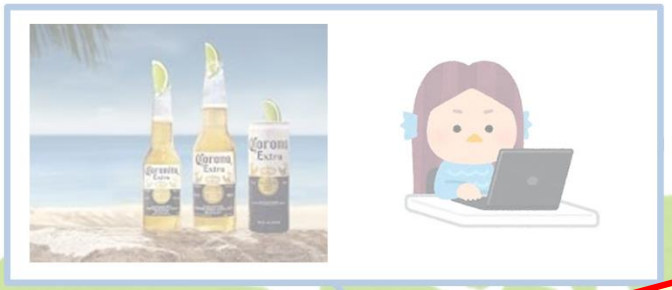
After コロナの目指す世界

- ✓ 物理（Real）環境に捉われない，仮想（Virtual）環境で働く世界
- ✓ 『Virtual Officeでの**円滑なコミュニケーション**』『業務SVの100%**Public Cloud**』『**AI**による業務効率化』『100%**電子決裁**』etc…



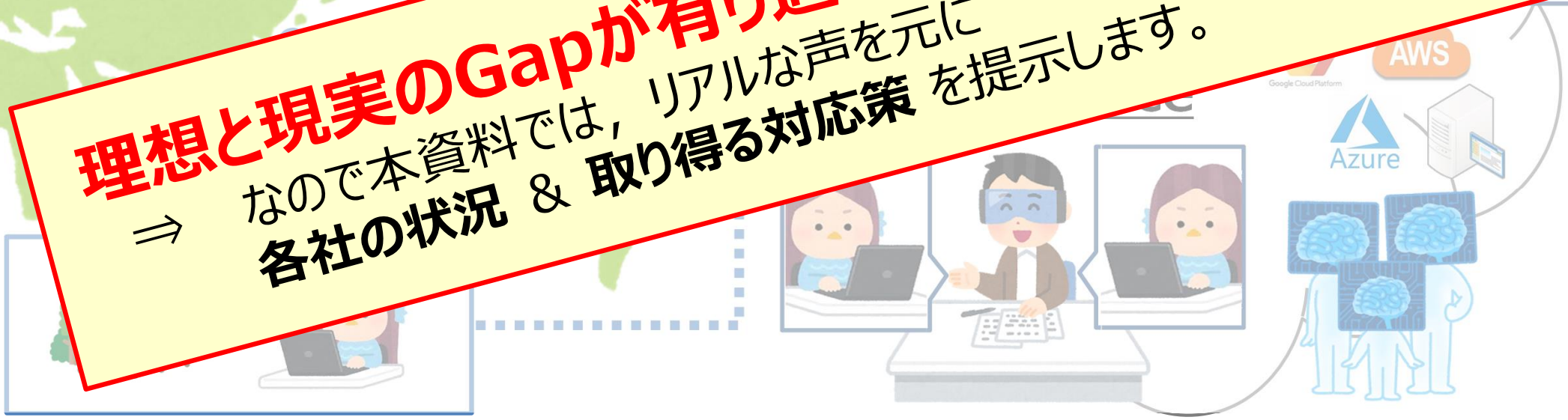
After コロナの目指す世界

- ✓ 物理（Real）環境に捉われない，仮想（Virtual）環境で働く世界
- ✓ 『Virtual Officeでの**円滑なコミュニケーション**』『業務SVの100%**Public Cloud**』
  『**AI**による業務効率化』『100%**電子決裁**』etc…



理想と現実のGapが有り過ぎて到底無理！！！！

⇒ なので本資料では，リアルな声を元に
各社の状況 ＆ **取り得る対応策** を提示します。



1.コロナ禍における各社での状況
ITインフラに求められるものは…？

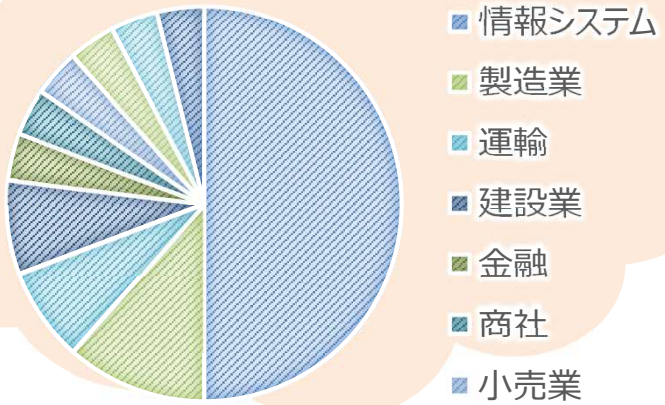
- ✓ 『Web会議』『VPN/VDI』『セキュリティ』など，ITインフラの出番も
- ✓ 実態の調査結果から課題を導出し，改善策を共有することで，今後のITインフラ（JUASメンバー）の立ち回りに貢献

アンケート
「テレワークによる変化」「ルールや制約」「環境」の3カテゴリで調査

課題定義/考察
共通課題や根本課題を導出

改善策の検討
After/Withコロナに向け，Best Practiceを検討

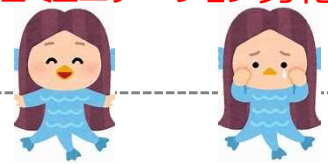
回答者：27名（半数が情報システム）



みなさま
ご回答ありがとうございました！

各社状況の概要

	カテゴリ	アンケート結果サマリ
1	テレワークによる変化	✓ テレワークは**大多数の企業が導入** ✓ オペレーション作業や現物確認，客先常駐作業など，出社ケースも多数 ✓ 作業効率は良し悪し双方あり（例：無駄な会議削減，コミュニケーション劣化） ✓ コロナビールは殆どの人が好き！！
2	ルールや制約	✓ 勤怠管理に関する制約が多数 ✓ 『メールの添付禁止』や『ローカルに保存しない』等，**セキュリティの制約**も散見 ✓ テレワーク時の端末は90%以上が会社貸与 ✓ 回線費用や光熱費は75%以上が自己負担（逆に，一部では現物支給アリ）
3	環境	✓ Web会議では**Zoom，Teams**が主流 ✓ **リモート接続はVPN**が多く，次いでVDI，RDP ✓ 回線逼迫も発生しており，30%が1.5~2倍の帯域に増強



以降のスライドで，**アンケート結果を深堀り**（課題定義や考察，改善策）

アジェンダ

1.コロナ禍における各社での状況

2.テレワークよる業務等の変化

3.テレワークにおけるルール等

4.各社での業務インフラ環境

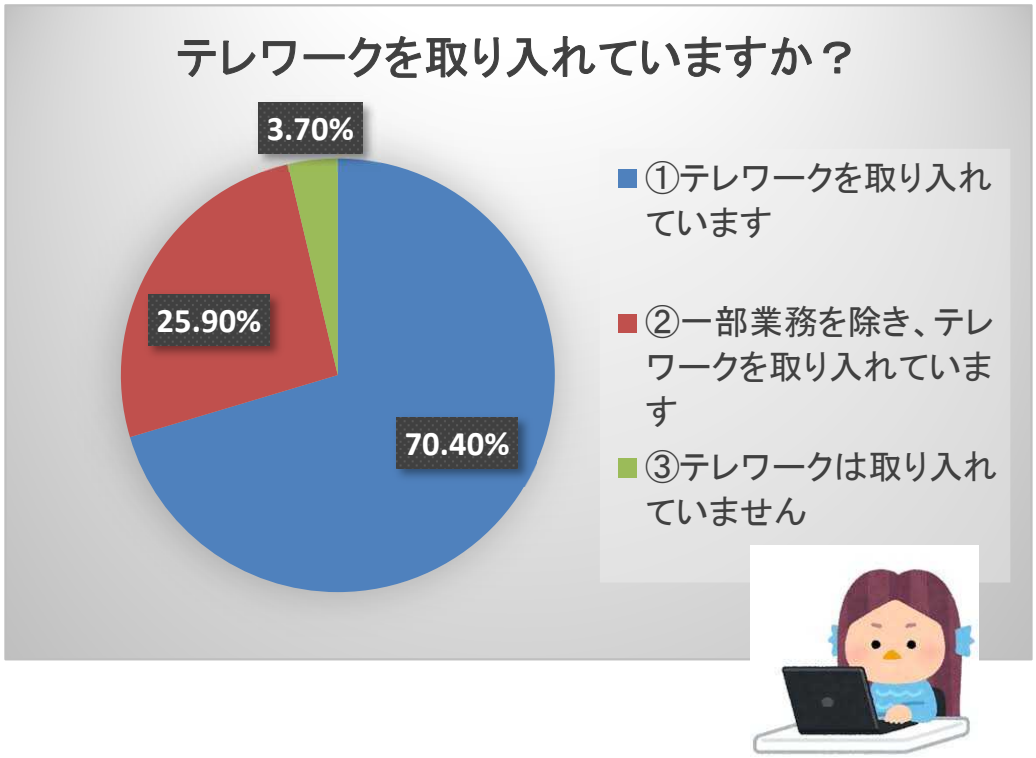
5.テレワークを推進していく上で必要な業務環境とは

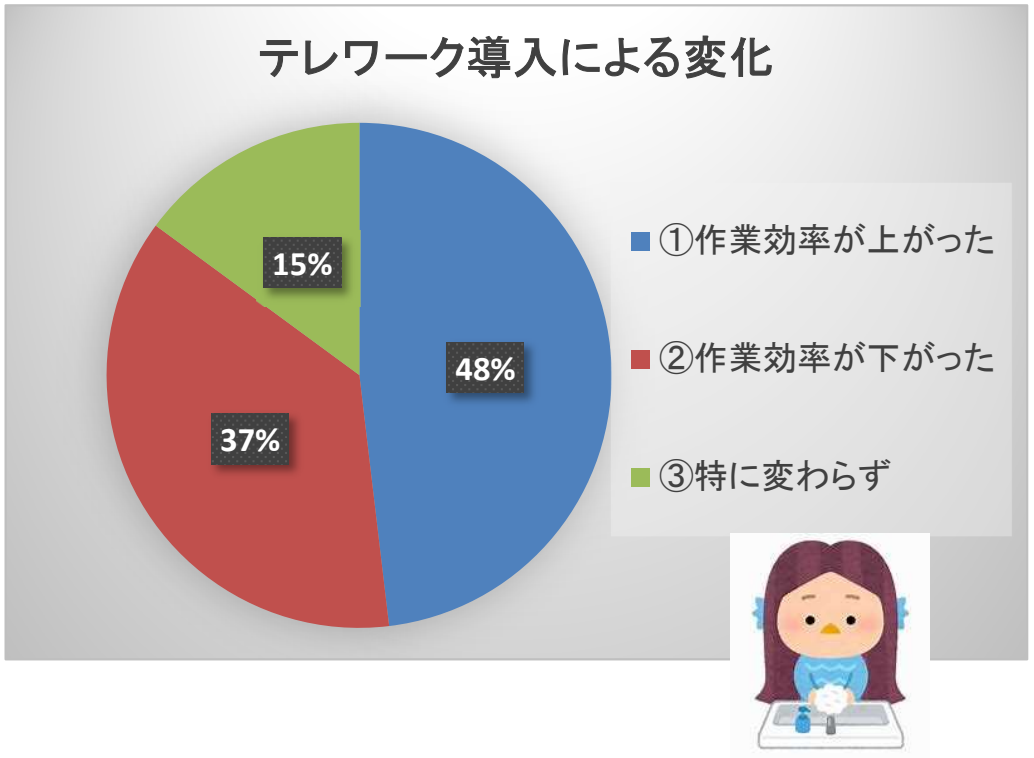
2.テレワークよる業務等の変化

各企業におけるテレワークの導入状況

- ✓ 多くの企業がテレワークを導入している
- ✓ テレワークの導入により約50%作業効率の向上を感じていることが分かった

○アンケート結果





2.テレワークよる業務等の変化

テレワークの導入効果

- ✓ テレワークにて作業に集中できることで個人ワークの効率が上がったという回答が多かった
- ✓ 近くに上司等がいないのでコミュニケーションやディスカッションには向いていないという意見が多かった ⇒ **各企業（業務）共通の課題**

効率が上がった、向いている

○個人ワーク
- ・提案書作成
- ・資料作成
- ・デスクワーク全般
- ・アイデア整理

○通勤時間、移動時間の軽減

○会議
- ・事前に資料確認できる
- ・準備の効率化

効率が下がった、向いていない

共通課題

○ディスカッション
- ・ブレスト

○コミュニケーション
- ・気軽な質問ができない
- ・状況把握が不明
- ・調整事がはかどらない

○現場作業
- ・オペレーション業務

○社内事務
- ・稟議、押印
- ・原本管理、原本搬送

2.テレワークよる業務等の変化

テレワーク導入における効率向上に向けて

- ✓ 各社共通課題のコミュニケーション効率を上げていくためにはリモート環境の準備が必要
- ✓ 現地作業や稟議・押印等は業務毎にシステム化等の準備が必要
- ✓ しかしテレワークにおいて、原本管理・原本搬送については困難である

効率が下がった、向いていないものをどうすればいいか

○ディスカッション
・ブレスト

○コミュニケーション
・気軽な質問ができない
・状況把握が不明
・調整事がはかどらない

→ Jamboadのようなツール
→ チャット・SNSの活用
→ Web会議での会話

○現場作業、
・オペレーション業務

→ リモート監視・リモート運用
→ RPAによる自動化

○社内事務
・稟議、押印

→ 電子決済

業務毎にそれぞれで準備が必要

・原本管理、原本搬送

アジェンダ

1.コロナ禍における各社での状況

2.テレワークよる業務等の変化

3.テレワークにおけるルール等

4.各社での業務インフラ環境

5.テレワークを推進していく上で必要な業務環境とは

各社の実態

✓ テレワークの導入にて各企業におけるルール等にも変化があった

労務規定

時差出勤やコアタイムの廃止

人事制度

75%変化なし
人事考課（評価）は悩みどころ

交通費

30%実費精算
60%が通常通り

新人研修

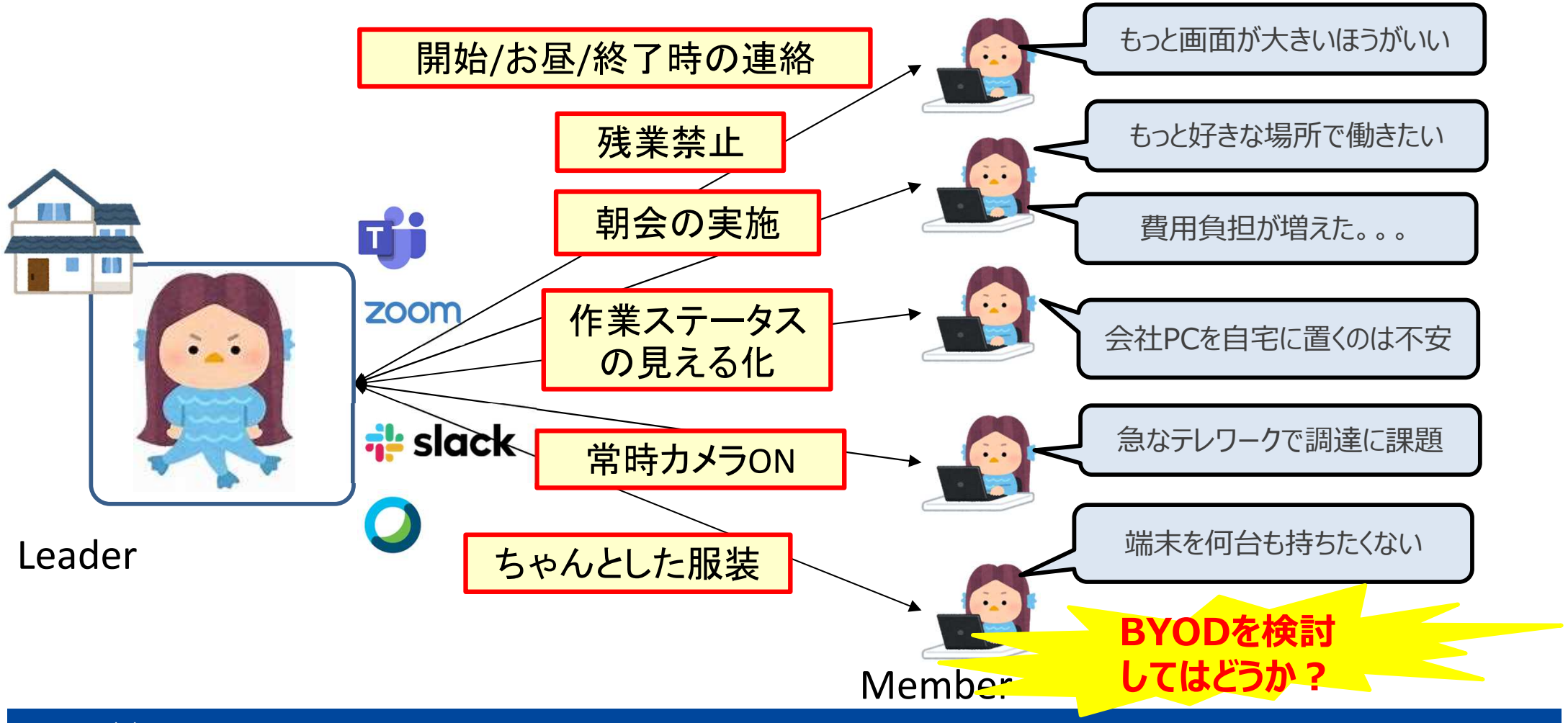
対面研修18%
オンライン・ビデオ研修約75%

懇親会

90%以上が懇親会なし

各社の実態

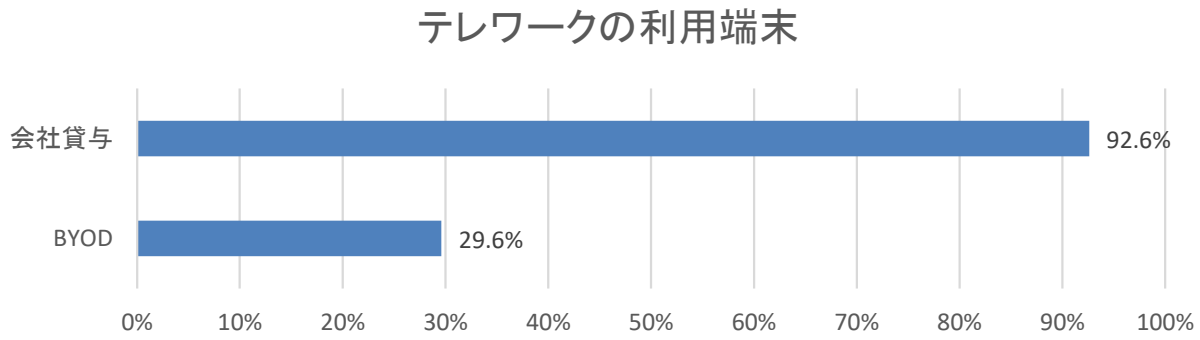
- ✓ 勤怠・コミュニケーションなど各社で種々のルールを設けて運営されている
- ✓ 一方、費用・情報の持ち出し(セキュリティ)に関しては課題があると考えられる
- ✓ 個人の作業環境に差があり、不満もでてきている　**⇒BYODの検討**

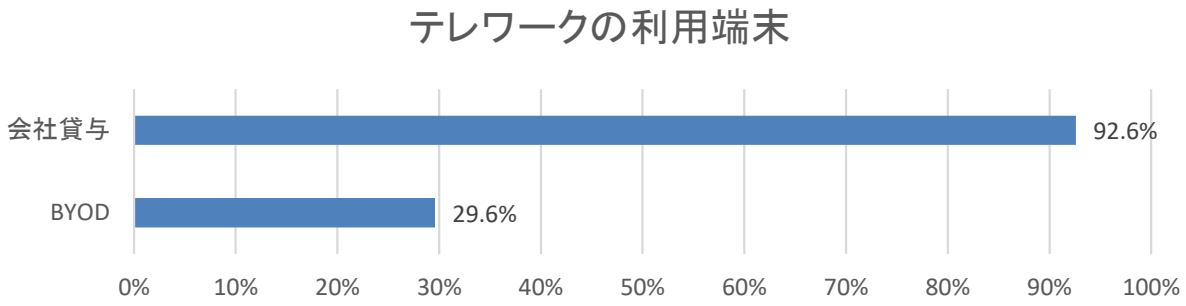


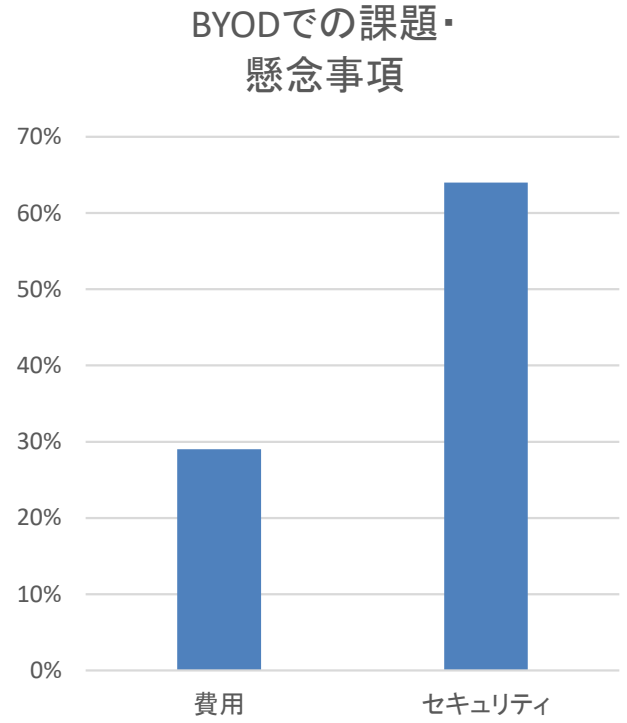
3.テレワークにおけるルール等

各社のBYODの現状

- ✓ テレワーク実施企業では9割が会社貸与の端末となっており3割しかBYODができていない
- ✓ 働く人/会社のそれぞれの要望満たせない形でテレワークを実施している
  ⇒各社、BYODを導入することでいつでも・どこでも効率的な業務を実現させたいのでは？
- ✓ アンケートの結果、主にセキュリティと費用面の課題で実施できていないのが現状
  ⇒情報の持ち出しルール、セキュリティ対策を取ったうえで個人が選べるようにしてみては？







BYOD活用事例は末尾付録参照

アジェンダ

1.コロナ禍における各社での状況

2. テレワークよる業務等の変化

3. テレワークにおけるルール等

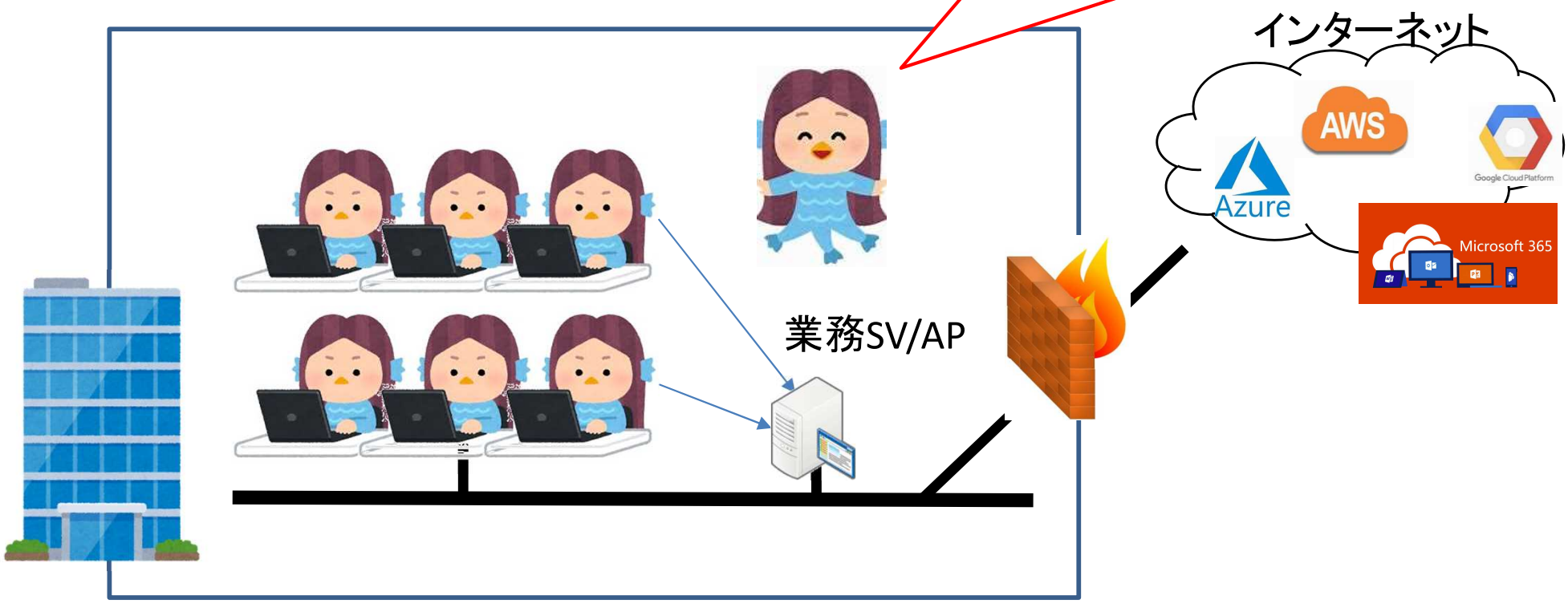
4.各社での業務インフラ環境

5.まとめ

4.各社での業務インフラ環境

Before コロナのインフラ環境

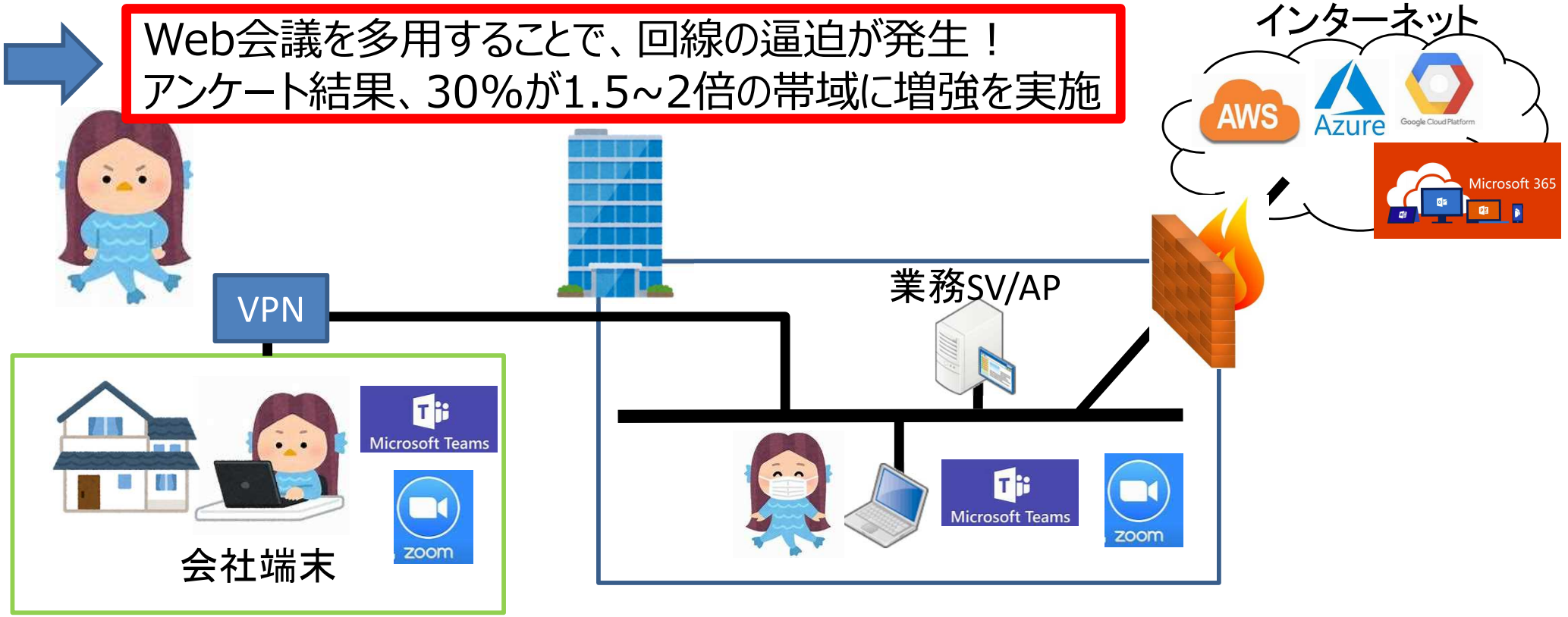
- ✓ 場所：会社
- ✓ 端末：会社端末
- ✓ 社内ネットワークへのアクセス：会社
- ✓ 会議形態：On-siteのF2F
- ✓ 業務SV/AP：社内（極一部Cloudへ）



With コロナのインフラ環境

- ✓ 場所：会社⇒**自宅**
- ✓ 端末：会社端末⇒**変化なし（会社端末のまま）**
- ✓ 社内ネットワークへのアクセス：会社⇒**自宅回線から VPN**
- ✓ 会議形態：On-siteのF2F⇒**Web会議（Teams･Zoom）**
- ✓ 業務SV/AP：社内（一部Cloudへ）

Web会議を多用することで、回線の逼迫が発生！
アンケート結果、30%が1.5~2倍の帯域に増強を実施



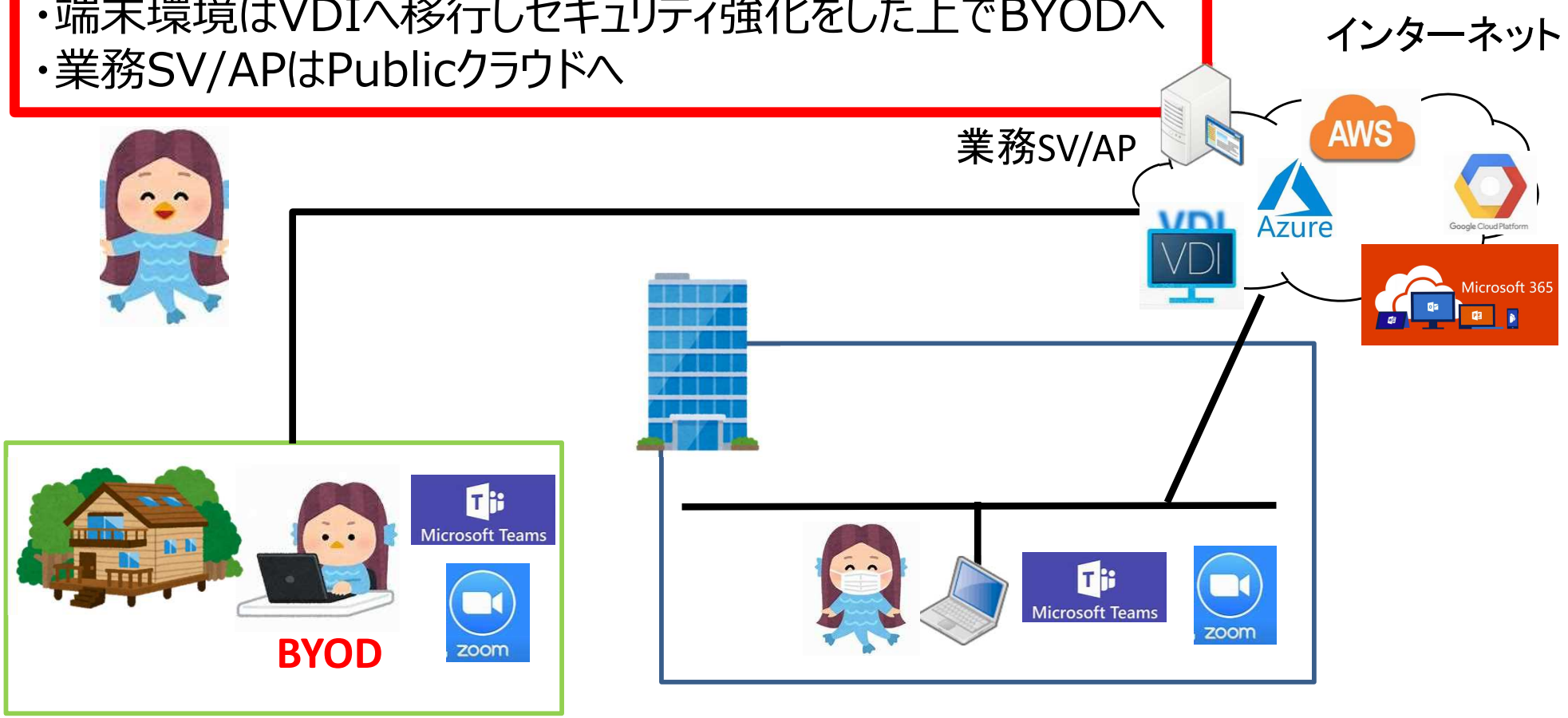
4.各社での業務インフラ環境

After コロナのインフラ環境

✓ 働く場所・端末にこだわらない
✓ 社内ネットワークの逼迫をなくす

⇒ 端末：会社端末⇒**BYOD+VDI**
業務SV/AP：社内⇒**クラウドへの移行**

・どこからでも誰でも仕事ができる・仕事をしやすい環境へ
・端末環境はVDIへ移行しセキュリティ強化をした上でBYODへ
・業務SV/APはPublicクラウドへ



4.各社での業務インフラ環境

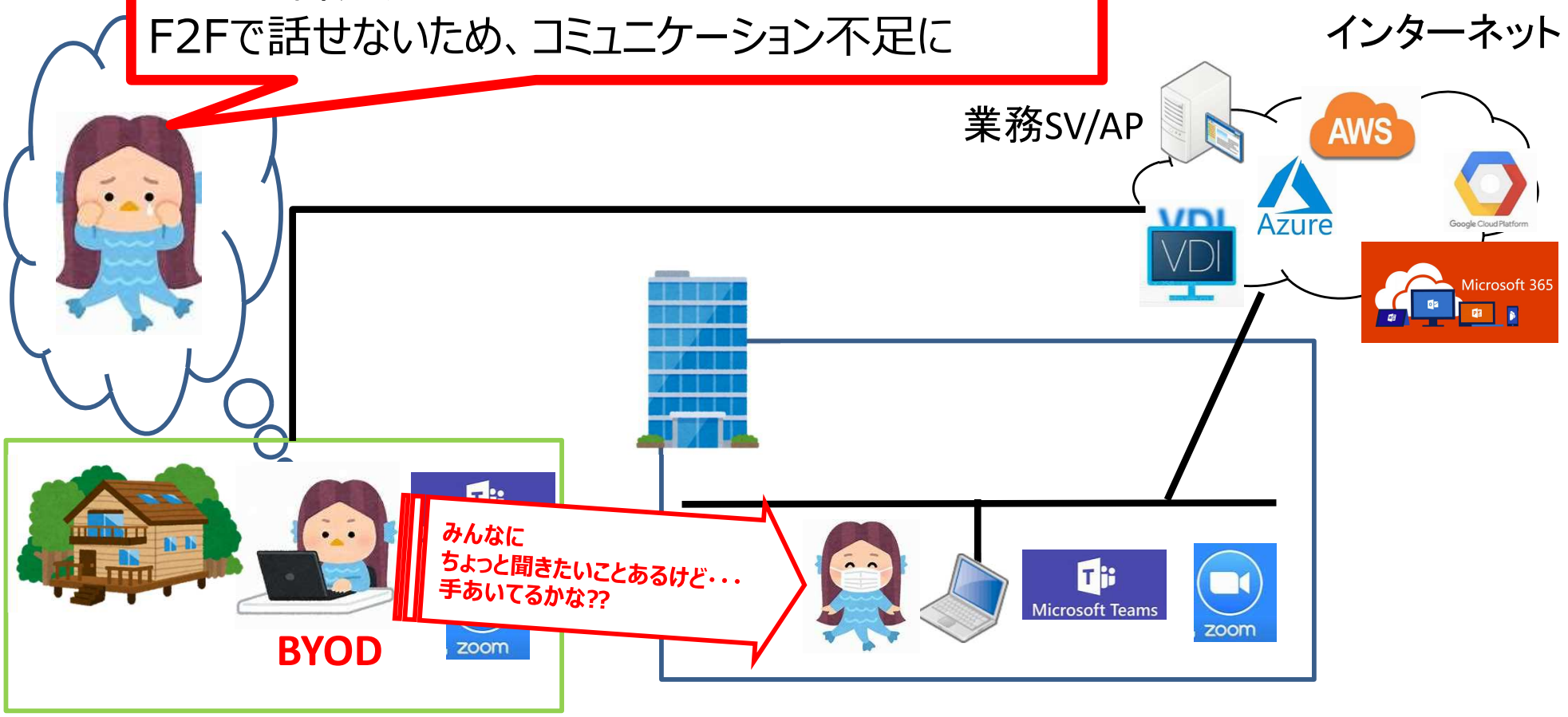
After コロナのインフラ環境

- ✓ 働く場所・端末にこだわらない
- ✓ 社内ネットワークの逼迫をなくす

⇒ 端末：会社端末⇒BYOD+VDI

Virtual Officeができれば変わるのでは！？

これでも課題が・・・・
F2Fで話せないため、コミュニケーション不足に



アジェンダ

1.コロナ禍における各社での状況

2.テレワークよる業務等の変化

3. テレワークにおけるルール等

4.各社での業務インフラ環境

5.まとめ

5.まとめ

テレワークを推進していく上で必要な業務環境とは

✓「とりあえずテレワークを導入したい！」 ➡ 対応策【短期】を確認！！
✓「Afterコロナでもテレワークを推奨したい！」 ➡ 対応策【中期】を確認！！

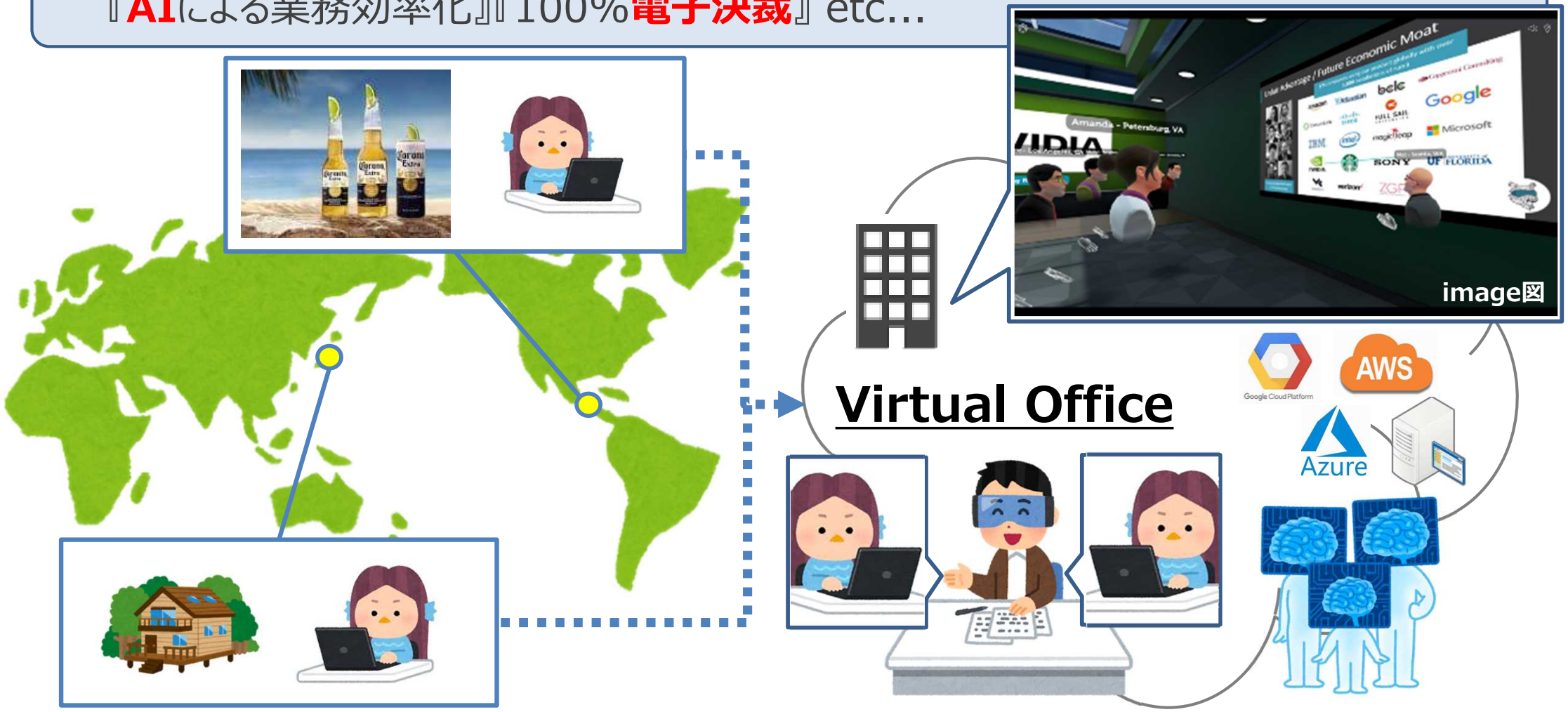
	カテゴリ	対応策【短期】	対応策【中期】
1	テレワークによる変化	✓ 個人ワークや会議への対応は不要 ✓ 気軽な会話・ディスカッション用にJamboadやチャットを提供すると◎	✓ RPAや電子決済の導入により、テレワーク普及率が向上する可能性
2	ルールや制約	✓ 勤怠管理の簡易ルールを設ける（成果の見える化,出退勤の連絡等） ✓ 情報の持ち出し(セキュリティ)を考慮した端末準備	✓ 費用とセキュリティに焦点を絞りBYODの導入を検討
3	環境	✓ 社内NWにアクセス可能なVPNを準備 ✓ コミュニケーションツール(zoom,teams等)を準備(契約)	✓ 回線逼迫対策としてVDIを検討 ✓ 業務SV/APをPublic化

さらに、After コロナの目指す世界はこんな感じ

再掲

JUAS

- ✓ 物理（Real）環境に捉われない，仮想（Virtual）環境で働く世界
- ✓ 『Virtual Officeでの**円滑なコミュニケーション**』『業務SVの100%**Public Cloud**』『**AI**による業務効率化』『100%**電子決裁**』etc…



さらに、After コロナの目指す世界はこんな感じ

再掲

JUAS

- ✓ 物理（Real）環境に捉われない，仮想（Virtual）環境で働く世界
- ✓ 『Virtual Officeでの**円滑なコミュニケーション**』『業務SVの100%**Public Cloud**』
  『**AI**による業務効率化』『100%**電子決裁**』 etc…

近年の情報(IT)技術革新を鑑みると，
あながち 夢物語 とも言い切れない…？

さらに、After コロナの目指す世界はこんな感じ

再掲

JUAS

- ✓ 物理（Real）環境に捉われない，仮想（Virtual）環境で働く世界
- ✓ 『Virtual Officeでの**円滑なコミュニケーション**』『業務SVの100%**Public Cloud**』
  『**AI**による業務効率化』『100%**電子決裁**』etc…

情報(IT)技術革新 ≒ インフラの出番

つまり…

我々が食い扶持に困ることは当分なさそう

（付録）
BYOD活用事例

✓ **以下のリスク軽減を目的にBYODを導入している企業もある**
－テレワークにて会社端末を持ち運ぶことによる紛失リスク・故障リスクの軽減
－仮想デスクトップを利用したリモート環境による情報漏えいリスクの軽減

BYOD導入にあたっては、環境面、ルール・制約面で以下の対応を取っている

〇環境
- データセンターに設置している仮想デスクトップ（VDI）環境を利用
- 仮想デスクトップからクライアント端末、外部媒体へのデータ保存不可
- 仮想デスクトップから自宅プリンタへの印刷不可
- 仮想デスクトップの端末操作ログを取得し、セキュリティ証跡管理運用を実施
- リモートアクセスにおける認証として、会社からRSAトークンを配布
  （接続先サーバURL＋ユーザID＋トークン＋デスクトップパスワードが必要）

〇ルール・制約
- 端末ログイン履歴と勤務管理を連動しており、時間外勤務等を制限
- 個人端末やネットワーク環境に関する費用負担なし（BYOD希望者制のため）

2020年度ITインフラ研究会

分科会A　活動報告

- 適性ＩＴコストを見極める

ユーザ企業、SIer双方の視点からITコストを斬る。小技から王道までの虎の巻。

2021年3月3日

ITインフラ研究会 分科会A
IT適性コストの見極め方チーム

テーマ選定の経緯

- 社内決裁を通すにあたり、コストの考え方やポイントが体系的にまとまった教材やガイドラインが存在しない。

- このため、
  - 運用費を削減する際、ベンダーと価格交渉をする際、優先順位、削減による影響、一般的なセオリーがわからない
  - コスト以外の要素の考え方（社内横断的な効果、人材育成）がわからない
  - ノウハウがあったとしても、担当メンバーに偏り、チーム内に共有ができない

- これを解決するために、情報システム部門によくあるシチュエーションで、こう考え、こう動けばいいのではないか、これまでの各社の経験をもとに虎の巻を作ることにしました。
  今回参加メンバーがユーザー３社、ベンダー１社のため、ユーザ、ベンダー双方の視点から、Win-Winの関係性となるアクションプランに仕立てています。

目次

1. こんな時に困っていませんか？

本書は以下シーンにおいて、ご活用頂けます。

システムEOL対応

- 構築コストが高い。この金額が妥当と言える？
- 今からじゃ単純リプレースしかできない。計画が遅い！！

→ シーン①

次年度ランニング予算の策定

- コストを10%落とせと言われても。削れるところってどこだろう。
- リソース（もの）、要員（ひと）どこから、手を付ければよい？

→ シーン②（もの）

→ シーン③（ひと）

新たな取り組み（新アーキ、技術の導入）

- 導入できれば、利便性や、システム運用負荷もさがる。
- PoCコストは妥当？コスト以外の効果は？

→ シーン④

2. 適正ITコスト＝要するに「決裁」を乗り越えたい！？

■決裁者目線で考える

投資／経費案件問わず、コスト以前に「**今、その方式で進める事の価値**」の確認が先ずあり、
内容が適正であれば「**より安価な調達／適正な売価**」などのも含めた、総合的な判断が下される。

ー多くのケースでは「額面／相場」に目を奪われがちだが、投資価値／意義の訴求こそ重要。
（通販比較のような「SI費用一覧」や相場など実質入手できない。あったら苦労しない）

■投資に対する適正価格は？

「適正ITコスト」を考える上でのフォーカスポイント

これらに答えられる
準備ができていますか？

会社/事業の方針

- 「今」それを進めるべき理由
- 「その方式」で実装／展開する理由
- 「それをやる自社／顧客」の価値

「やる」と
決まったら

投入コスト・金額の妥当性

- 金額の「内訳」を論理的に説明できるか
- 投入する、モノ・ヒト・サービスは適切か
- 外部調達は比較し「相対的に安価」か

3. シーン別攻略ガイド
サマリ編（１）基本的な考え方

シーン①：EOL に伴うシステムリプレース

1. 徹底したライフサイクル管理
- 検討期間不足から選択肢が限られ、コスト増に繋がりがち
- 計画の自由度、選択の幅を広げる

2. ベンダーへの提示要件の曖昧さの排除
- 曖昧さのリスクヘッジのためベンダーは過剰構成・タスクを提案しがち
- 要件、役割分担がきっちり握ることがコスト削減の近道

シーン②：次年度ランニング予算策定（HW/SWサポート費、利用料）

1. 無駄な保守の足切り
- 償却を終えるまで継続利用するのが基本(削減は難しい)
- 過去の保守サポート利用実績、環境変化の振りかえり
- 運用を担っている担当だからこそわかる無駄がないか、日々の地道な点検が重要。

シーン③：次年度ランニング予算策定（保守要員、オペレータ費）

1. 顧客と痛みを分かち合う構造へ
- サービスレベルを落とさずに提供価格のみを落とそうとしがち
  →現場の疲弊を招く
- コストとともにどのサービスを落とすのか顧客に判断を頂くべき
- この大原則は崩してはいけない

2. 無駄な保守の見直し、オペレーション業務効率化
（シーン②と同様）

シーン④：次世代アーキ・技術導入および、PoC

1.取り組みの先にある価値
- PoCではなく、取り組みの先にある価値が重要
- 決裁者は直接的なビジネスへの貢献以外に、間接的な効果として会社全体の目線で組織、他PJ、今後の取り組みへの効果や、要員育成への効果を包括的に見る。決裁者目線で効果を語ることが重要。

2.PoCは捨て金ではない
- 選択肢の絞り込み、ノックアウト要素、将来的損失の洗い出し
- 先にある価値、実現確度の最大化のために必要な投資

3. シーン別攻略ガイド
サマリ編 （２） アクション

シーン①：EOL に伴うシステムリプレース

1. リプレースタイミングの見極め
- ・複数システムの同時リプレースによるボリュームディスカウント
- ・ITサプライヤーの決算時期の把握（価格交渉の優位性の確保）
- ・要件調整による一部機能の縮小、別システムへの統合

2．委託先ベンダの選定
- ・メーカーによる後方支援具合(導入製品のプレミアパートナー等)
- ・PM評価、PM自身からPJ方針を説明(営業だけが優秀な場合あり)

シーン②：次年度ランニング予算策定（HW/SWサポート費、利用料）

1. 第三者保守への切り替え
- ・運用安定化によるSW保守の第三者保守への切り替え
  (万が一の場合、回避不能な脆弱性・不具合リスクあり)

2. 無駄なオプション機能の廃止
- ・導入後利用しなくなったオプション機能等の廃止

3. HW/SW保守提供比率の見直し
- ・前年度の運用実績からサプライヤーと保守費、SLAの見直し

4. サービスレベルの見直し
- ・稼働時間、可用性、スペック、利用者が少ないサービスの見直し

シーン③：次年度ランニング予算策定（保守要員、オペレータ費）

1. サービスレベルの見直し
- ・監視時間、保守グレードの見直し、無駄なレポートの廃止

2. 運用業務の自動化、メニュー化
- ・定期定型業務のRPAによる自動化(費用対効果が高いところから)
- ・メニュー化による業務効率化、顧客も必要サービスのみに限定可

3. リモート保守の活用
- ・オペレータ業務のリモート化。テレワーク、パンデミック、災害時のオペレーション業務のBCPが確立。個別体制の確保が不要となる。
- ・ITサプライヤによる遠隔保守。一次切り分け等の中間業務の削減。

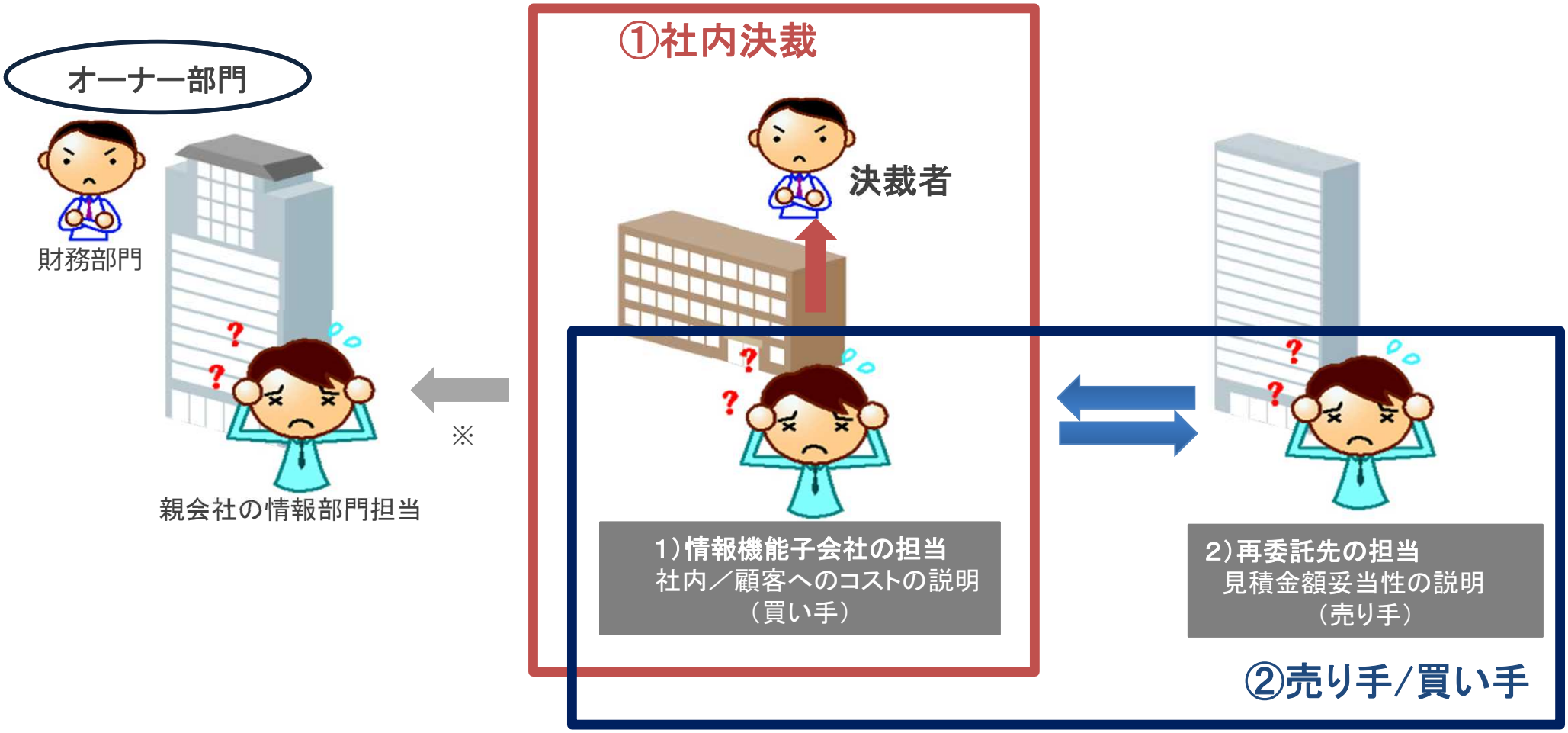
シーン④：次世代アーキ・技術導入および、PoC

1.　自社におけるインフラ戦略との適合
- ・自社のインフラ業務のコア・ノンコアのすみ分け
- ・サーバレス、SaaS、コンテナ、IaaS、HCI、オンプレどこに進むか

2．　効果を示す
- ・短期的、直接的な効果。品質、コスト、納期、セキュリティ面
- ・中長期的な効果。他システム、PJ、他部門、グループ各社
- ・全体最適に繋がっているか
- ・人材育成、ナレッジ蓄積への効果

4. ITコストを語るための2つの目線

今回は①社内決裁、②売り手/買い手という「2つの目線」でIT適正コストを考えます。



※社内決裁とオーナー部門決裁の評価観点は同様とする。

5. 新規／継続(共通)
シーン①:EOL に伴うシステムリプレース ： シーン

リプレイス | 保守・利用料 | 保守員オペ費 | 新技術・PoC

システムEOLに伴い、システムリプレース計画を社内決裁に付議しました。構成・費用はSierと協議を重ね、納得の内容に仕上げています。

決裁者/
経営者

単純リプレースなのに高い。
もう少し削減できる要素はないのか？

さぁ、どう答えますか？

ユーザ担当者
（買い手）

Sier/製品ベンダー
（売り手）

5. 新規／継続(共通)
シーン①:EOL に伴うシステムリプレース ： 考え方

リプレイス | 保守・利用料 | 保守員オペ費 | 新技術・PoC

①社内決裁

■まずは目的と効果、そこにかかる費用を明確に！！
- 決裁者は導入効果や費用対効果が見えないモノ(システム)には投資を渋るもの。まずは目的と効果、費用を明確にする必要がある。
- 各機能やサービスにかかる費用がわからないことには、決裁者は判断できない。

■導入製品は自社業務にマッチしているか？
- 数多ある製品の中で自社の業務にマッチする製品を選定しないと、不要な機能へのコストが膨らんでしまう。
- 製品の事前調査は、十分におこなう必要がある。

■徹底したライフサイクル管理が、計画の自由度、選択の幅を広げる
- EOLに伴うリプレース対応において、検討期間が十分に確保できず、結果手段や選定製品が限られてしまうことがありがち。
- 期限が迫っているためという理由で選定した手段、製品では、得てして社内決裁で理解を得ることは難しく且つ、リプレース費も高くなってしまう場合が多い。
- ライフサイクル管理の徹底がキモ。

5. 新規／継続(共通)
シーン①:EOL に伴うシステムリプレース ： 考え方

リプレイス | 保守・利用料 | 保守員オペ費 | 新技術・PoC

②売り手／買い手

■もの代:必要な性能、機能、冗長要否の見極め
- インフラコストを大きく左右するものは、H/Wスペック(CPU、メモリ、ディスク)など性能面、S/W機能・オプション有無、環境数、信頼性(冗長化、バックアップ要否)。
- 本当に必要なシステム要件の見極めが必要最低限の投資となるか左右する。

■人代:工数以外の要素(個人能力、PM力、実績)も含めて判断せよ
- 構築費用は必要となる工数で決められるのが一般的。但し、個人スキルやベンダー毎のノウハウも加味するため、単に工数だけで判断することは非常に難しく、様々な切り口での見極めが重要。
- また、ミドルウェア構築では工数ではなく、作業メニューとして提示するベンダーもある。メニューの場合、要員の出来不出来で左右されず、アウトプット、構築業務も明確化されているため、こういったパターンの採用を検討するのも良い。

■ベンダーへの提示要件の曖昧さがコスト増を招く
- ベンダーに対し、曖昧な要求や「オススメで」という要望をした場合、やや過剰な構成で提示されることある。これはベンダーの立場からすると、後から「性能がでない」などのクレームを避けるため、バッファを載せた結果。
- 構築に関しても考え方は同様で、「全部お任せで」では、同じく過剰な工数が出てくることが多い。
- ユーザは自社の運用担当者やアプリ開発者と協議し、必要なリソースや機能を可能な限り洗い出すことが重要。
- 自社でできることを明らかにし、ベンダーへの委託内容やスコープを定義することで、コストもより適正化され、妥当性確認や調整相談もしやすくなる。

4. 新規／継続(共通)
シーン①:EOL に伴うシステムリプレース ： アクション

①社内決裁

＜アクション＞

1. **複数社による費用、機能、提供サービスの比較**
   比較することにより、提案の妥当性や製品のトレンド価格もわかるため判断しやすくなる。

2. **コンサルティングサービスの利用など、検討業務の社外委託**
   ・自社のみで製品調査、選定が難しい場合は、社外のシステム会社に依頼をすることも検討する。
   ・自社サービス、製品を保有している会社では、フラットな選択ができない可能性やベンダーロックを考慮すると、コンサルティングサービスを提供しているシステム会社(コンサル会社、独立系SIer)を選択すると良い。

3. **余裕を持った計画の策定による自由度・柔軟性の向上**
   ・システムライフサイクル管理の徹底により、余裕を持ったリプレース計画が策定でき、結果、自由度の高い計画の策定が可能となる。
   ・関連システムのリプレース時期を合わせることで開発費用を削減、製品価格調整がしやすい時期(決算時期)を狙うことでHW、SW費を抑えることも可能である。
   ・要件調整による一部機能の縮小、リリース時期見直しも検討する。
   ・システム全体のロードマップ策定
   ・関連システムとのリプレース時期調整
   ・購入時期調整、リプレース範囲の見直し

4. 新規／継続(共通)
シーン①:EOL に伴うシステムリプレース ： アクション

リプレイス | 保守・利用料 | 保守員オペ費 | 新技術・PoC

②売り手／買い手

＜アクション＞

1. インフラ費用 (H/W)
   - ・必要なリソース(CPU/メモリ/ディスク)のサイジング
   - ・利用な環境(本番、検証、開発)の確認
   - ・構成(冗長化)の検討
     →あわせて適正化の検討
     - ・検証/開発環境はリソースや冗長要件を抑える

2. インフラ費用 (S/W)
   - ・必要な機能にあわせた製品の選定
     - – 基本+オプション型:要求機能少ない場合は優位
     - – オールインワン型:多い場合には、こちらがよい
   - ・適切なライセンス調整
     - – ライセンス定義を確認依頼(ベンダーに説明依頼)
     - – 例えばユーザライセンスがあれば開発環境は
       そちらにするなどの調整

3. 依頼作業の洗い出し
   - ・ユーザでできることの整理
   - ・ベンダーに依頼する内容/スコープを明示(文書化)

4. 委託先ベンダーの選定
   - ・価格競争力のあるベンダー
     - – ベンダーのHP(参入年数/実績/事例)
     - – 提案資料に明記依頼
     - – メーカと協調して動いているか
       緊急時の対応

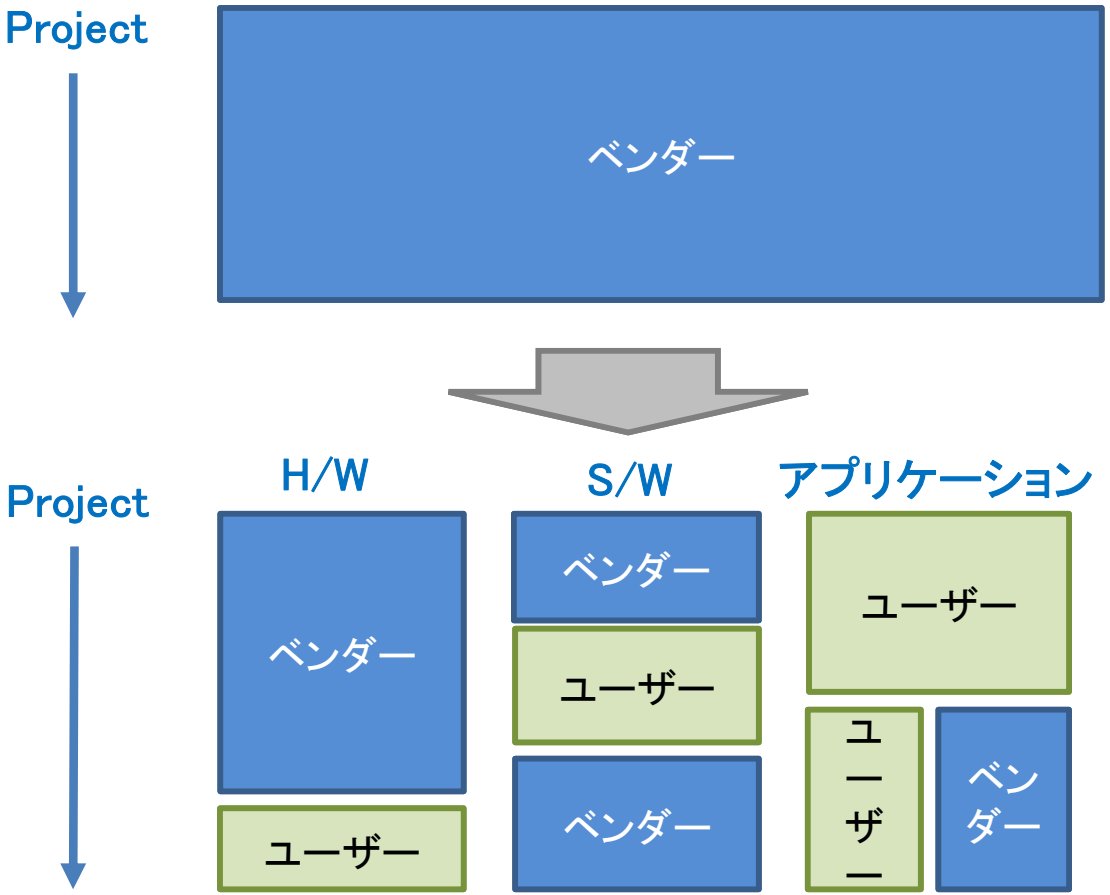
5. 構築費用の見極め

A) スキルセット確認例
- ・経験年数
- ・同規模案件の実績
- ・社内での役割、立場
- ・プロジェクトマネージャ(PM)の経歴確認

B) 妥当性判断例
- ・プレゼンの場にPMに同席依頼
  例えば「プロジェクト遂行方針」を説明してもらい、
  そのヒトの姿勢/思考/想いを知る

②売り手／買い手

■コスト最適化には、ユーザとベンダーの役割分担が重要



・HW/SW構築、開発を一括委託の場合、
高コストになりがち
・コストの妥当性判断も難しくなる

・リプレースではユーザが担う部分も意外と多い
・領域やフェーズ毎に役割を明確化することに
より、コストの削減は可能。
・ベンダー担当の見極めは前頁参照

→これにより、適正なコスト算出へ

5. 継続　:投入リソース・金額の妥当性
シーン②:次年度ランニング予算策定(HW/SWサポート費、利用料):　シーン

来年度のランニング予算提出のシーズンとなりました。
その中でもHW、SW、利用料周りのコストについて問われました。

決裁者/
経営者

顧客の来年度IT予算(ランニングコスト)が厳しく〇%の
削減要請が来ている、HW/SW/利用料等に関する
経費予算の妥当性を説明してください。

さぁ、どう答えますか？

ユーザ担当者
(買い手)

Sier/製品ベンダー
(売り手)

5. 継続　:投入リソース・金額の妥当性
シーン②:次年度ランニング予算策定(HW/SWサポート費、利用料):　考え方

①社内決裁

■HW/SWは償却を終えるまで
投資したHW/SWは償却を終えるまで継続利用するのが基本。
これを踏まえつつ、HW/SW/利用料に関してどのコストが削減できるのかを考える。

■HW/SW保守の無駄は運用担当しか見つけられない
保守契約更新時に前年度と同じコストであれば、そのまま保守更新をしてしまいがち。一方で、保守内容を理解し内容を精査できているでしょうか。過去の保守・サポート利用実績、環境の変化なども含めて振り返り、保守・サポート内容に過不足が無いのか、システムライフサイクルの観点でバージョンアップ権など不要なものが無いか、などの精査が必要。運用を担っている担当だからこそ判る無駄を抽出してください。

■利用料関連のランニングコストの無駄を見つける
クラウドなどの従量課金モデルでは、インスタンスの停止などでの課金停止の処置や、利用者が少ないサービスを見極めてクローズの検討するなど、日頃の請求内容も精査し、コストカットできる部分を見つける必要があります。

―これらは予算時期に入ってからの点検では間に合わないため、上期振り返りなど
タイミングを定め、運用担当者目線での点検を行う事が重要(日頃からの備え・着眼)

5. 継続　:投入リソース・金額の妥当性
シーン②:次年度ランニング予算策定(HW/SWサポート費、利用料):　考え方

②売り手／買い手

■サポート費内訳の現状理解
まずはサポート費内訳を正しく理解することが重要。H/W筐体及びS/Wライセンスのサポート費用が基本ではあるが、
オプションやベンダーからの付加価値サービスなどもある。売り手/買い手ともに共通認識を持つ。

■調整に向けて、お互いに準備する
サポート費の内訳を確認後は、調整できる範囲を、売り手/買い手ともに検討する。
例えば、H/W保守数年保守が締結されていることが多く途中の変更は難しい。
S/Wやオプション/付加価値サービスなどの年単位などは、調整対象の選択肢にはなりえる。
またクラウドを利用の場合には稼動時間が大きな要素であり、運用方針踏まえての再考も必要となるだろう。
ただ、コスト抑制が全面に出すぎで、むやみな削減が多くなり、その後のサポート運用に支障がでては本末転倒。
ユーザ側も自社に本当に必要なサービスを慎重に検討しつつ、現状のサポートとの適合性の見極めが必要。

＜ベンダー＞
- 内訳の中で、年毎に見直しできる内容の提示
- 既存のサポート内容の代替案(コスト削減/効率化)の準備

＜ユーザ＞
- 自社で本当に必要なサービスの棚卸し
- 新たにリクエストしたいサービスの検討

5. 継続　:投入リソース・金額の妥当性
シーン②:次年度ランニング予算策定(HW/SWサポート費、利用料):　アクション

①社内決裁

＜アクション＞

1. 保守・サポート・対応時間の縮小
   ・保守・サポート内容を改めて確認し、これらの利用実績や、実際に求められる保守・サポートレベルとの乖離が無いかを点検する。変更する場合は予め顧客と合意し、次年度予算の妥当性を示す。

   ・可用性レベルの見直し
   ハードウェアの冗長構成あるいは保守範囲を割り切ってシングルとし、保守対象自体を削減するなどのアプローチも考えられる。これらは、過去の故障実績、障害時の業務影響度、利用ユーザ数等を踏まえて検討。

2. クラウド課金モデル目線の点検
   クラウド上のインスタンス起動時間の見直し・リソース削減などを確認し、利用料周りの妥当性を示す。

3. 利用実績(リソース・通信量)の点検
   実際の通信量・利用サービス・確保したキャパシティの過不足状況を確認し、適正な契約への切替を検討。

4. 第三者保守への切替
   保守更新のタイミングなどで、第三者保守などの検討を行う。保守・サービス内容、金額などの比較を行い保守契約先の再評価を行う。

5. 継続　：投入リソース・金額の妥当性
シーン②：次年度ランニング予算策定（HW/SWサポート費、利用料）：　アクション

②売り手／買い手

＜アクション＞

1. サポート費用内訳、調整に向けた事前準備
   ・前頁の考え方参照

2. サポート内容の妥当化協議
   具体的な調整例
   ・ H/WやS/Wのオプション機能
   　– 当初必要と考えられ導入したが、その後使われなくなったケースの見直し
   ・付加価値サービス
   　– 監視の仕組み/クラウド稼働時間 などでは、その継続是非や代替案の検討
   ・保守の提供比率
   　– 筐体/ライセンスの初期費用と比べると、保守費用は下げにくい傾向がある。
   　– 一般的には導入構成の〇%となっているケースが多いが、例えば運用フェーズが順調に推移し、事例化が可能であればベンダー側にもWelcomeな状態。こういった働きかけで比率調整を相談を実施する。

3. 他ベンダーへの見積相談（ユーザ側）
   ・保守提供比率や付加価値サービスは、ベンダーによって異なる。
   ・保守ベンダーが変わるリスクはあるが、別の見解を得るという観点では相談してもよいだろう。

6. 継続　:投入リソース・金額の妥当性
シーン③:次年度ランニング予算策定(保守要員、オペレータ費):　シーン

来年度のランニング予算提出のシーズンとなりました。
その中でも保守要員、オペレータ要員コストについて問われました

決裁者/
経営者

来年度保守要員、オペレータ要員ランニングコストが
なぜこんなにかかるのか？下げられないか？

さぁ、どう答えますか？

ユーザ担当者
(買い手)

Sier/製品ベンダー
(売り手)

6. 継続　:投入リソース・金額の妥当性
シーン③:次年度ランニング予算策定(保守要員、オペレータ費):　考え方

①社内決裁

■自社の委託費負担の考慮

保守要員/オペレータのコストを削減を考える場合、自社のビジネスパートナ委託費の考慮が必要。このケースでは、ビジネスパートナを縮小(人減らし)し、直接的に委託費を削減するか、人を減らさずに顧客との契約で運用業務を削減しつつ、そこで空いた時間を別業務へ振り分けると言った対応がセットで必要となる。

■ビジネスパートナの再考

保守要員・オペレータ費でビジネスパートナへ委託している場合は、委託先のコスト(単価及び人数)の見直しや稼働率・パフォーマンスの評価が必要。
(但し昨今はIT人材不足であり、オペレーション要員の追加は容易ではない。加えてコロナ禍により、データセンタ常駐など「出勤」が必要となる業務が好まれない傾向にあり、常駐員の確保は今後も困難になると考えられる)

■人件費を削減したからといって、提供価格を落としてはならない。

顧客へ提供する運用・保守サービスに対価が支払われる。よって、若い担当或いは、より安価なビジネスパートナとの契約により人件費(委託費)を削減出来たとしても、これをダイレクトに顧客への提供価格削減としてはならない。
提供サービスの削減の顧客合意とセットで初めて運用コストの削減が可能となる、という大原則を守るべき。

サービス削減なしに運用費だけを落とすと、人員が入れ替わった際に原価と売価のバランスが維持できなくなるリスクを自社が背負う事になり、後からの運用コストの値上げなどはまず不可能と考えた方が良い。

6. 継続　:投入リソース・金額の妥当性
シーン③:次年度ランニング予算策定(保守要員、オペレータ費):　考え方

②売り手／買い手

■受注者だけが負担することは避ける
コスト削減要請を受けたとしても、提供価格を安易に下げるべきでない。コストと共にどのサービスを落とすのかを顧客に判断頂くべき。あくまでも顧客に痛みが伴う構造へ。

■サービス提供内容の見直し
保守対象の設備すべてに対して同一のサービスレベルとなっていることで、過剰なサービス提供となっている可能性がある。顧客と提供者間にて設備ごとのサービスレベルや責任分界点を明確にすることで、顧客の求めるサービスを提供し、やらなくていいことを明確にする。

■運用業務の効率化
サービス提供にあたり必要な人件費ではあるが、業務コストの削減をしないと利益率も上がらず、他社との競争に負けてしまう。運用業務の作業工数削減などの効率化を図る施策も検討する。

6. 継続　:投入リソース・金額の妥当性
シーン③:次年度ランニング予算策定(保守要員、オペレータ費):　アクション

①社内決裁

＜アクション＞

1. 先ずはサービス内容の縮小範囲を顧客と合意する
   コストを削減する分、サービスも当然縮小される。どのサービスをカットすることで、いくらの削減となるのか顧客と合意すること。(単純な値下げはご法度)

2. サービス削減した場合、運用要員は別の業務へアサイン
   顧客とサービスをカットした場合、従来そこに割り当てられていた要員(常駐パートナなど)は別の業務に割当、稼働率を落とさないようにする。(業務が減り遊ばせた場合は自社のコストが無駄となる)

3. 最悪保守要員を〇名カットせざるを得ない場合、
   常駐要員の場合、1名単位での削減となるため、残された人員で実質的に対応が可能なのかの確認を行う。
   データセンタの常駐要員などを削減対象とする場合、外部のオペレーションサービスなどとコスト比較を行う。

4. あまりに無理強いな要員コストのカットの場合
   その契約を「受けない／撤退」という決裁者側の判断を求める。(現場が苦しむだけです)

6. 継続　:投入リソース・金額の妥当性
シーン③:次年度ランニング予算策定(保守要員、オペレータ費):　アクション

②売り手／買い手

＜アクション＞

1. 顧客と合意のもと、システム毎のサービスレベルの見直し
   - ・監視時間のサービスレベルを落とす
   - ・保守グレードを落とす
   - ・実質活用度合いの低いレポートサービスの廃止

2. 運用業務のサービスメニュー化
   顧客は必要なサービスを選択することができ、過剰なサービス提供を抑制する。

3. 定期定型業務のツール/RPA化による作業工数削減
   全ての業務に対しての適用はなかなか進まないため、作業量、頻度が多い業務を部分的、段階的に実施するなど対象範囲を検討する。

6. 継続　:投入リソース・金額の妥当性
シーン③:次年度ランニング予算策定(保守要員、オペレータ費):　アクション

②売り手／買い手

＜アクション＞

4. リモート保守の活用

1)オペレータによるリモート保守:監視要員のテレワーク、パンデミックや災害時への対応が可能となる。
　効果:コスト観点ではテレワークの効果になる

2)ベンダーへの自動通報:オペレータからベンダーへのエスカレーション業務の効率化、初動の迅速化。
　効果:コストメリットより初動の迅速化がメイン
　費用:ベンダーとの保守費用に監視分が追加されるので高くなる可能性がある

3)ベンダーによる遠隔保守(診断、調査):オペレータによる状況調査、ログ採取、ベンダーへのエスカレーションの効率化。
　効果:効率化された部分の工数が削減できる
　費用:ベンダーとの保守費用がオンサイト対応がなくなるので安くなる可能性がある

セキュリティ的に社内→社外(通報)はハードル低、
社外→社内(保守、診断)はハードル高。

7. 新規・更改　:時期・方式・価値の妥当性
シーン④:次世代アーキ・技術導入および、PoC：　シーン

サーバレス、構築自動化、API連携など、新技術・次世代アーキテクチャを導入し、ビジネスの変容にクイックに応えられるITインフラ環境を企画した。

決裁者/
ユーザ

・運用するための体制、コスト、全体構成・運用方式
　との整合性は？
・PoCはやる必要はあるのか？

さあ、どう答える？

ユーザ担当者

7. 新規・更改　:時期・方式・価値の妥当性
シーン④:次世代アーキ・技術導入および、PoC :　考え方

①社内決裁

■取り組みの先にある実現したい事が大切
- まず自社のインフラ戦略とマッチしているかを確認する。マッチしていれば問題ないが、マッチしていない、もしくはインフラ戦略自体が存在しない場合、<u>コスト以前</u>に、この取り組みの意義・必要性、導入の先にある効果を明確にする必要がある。
- PoCはPoC自体が重要ではなく、先にある効果、何を実現したいかが重要。
- 決裁者(経営者)は、この取り組みを行うことにより、直接的なビジネスへの貢献や、間接的には、今後の広がりや、ナレッジの組織全体への浸透、若手育成への効果を包括的に見る。決裁者目線で効果を語れるかがポイント。

■取り組みの意義、必要性

①価値の妥当性:
- コスト、品質、提供時間、ユーザビリティの改善などの直接的な効果と、社員育成、ナレッジ蓄積、チーム横断による組織活性化など副次的な効果
- 短期的な効果と長期的な効果、別プロジェクト、他組織への好影響など

②時期の妥当性: 今なぜやる必要性があるのか

③方式・手段の妥当性:構成、方式、進め方、手段は最も効率的、合理的か。

■PoC、技術検証コストは捨て金ではない

PoC、技術検証は、ノックアウト要素の洗い出しや、選択肢の絞り込みであり、将来的な損失、手戻りを防ぐための投資であるため、捨て金ではない。プロジェクト開始後に致命的な問題が発生し、投資コストを全額回収できなくなる事態に陥らないよう必要な投資と言える。

7. 新規・更改　:時期・方式・価値の妥当性
シーン④:次世代アーキ・技術導入および、PoC :　アクション

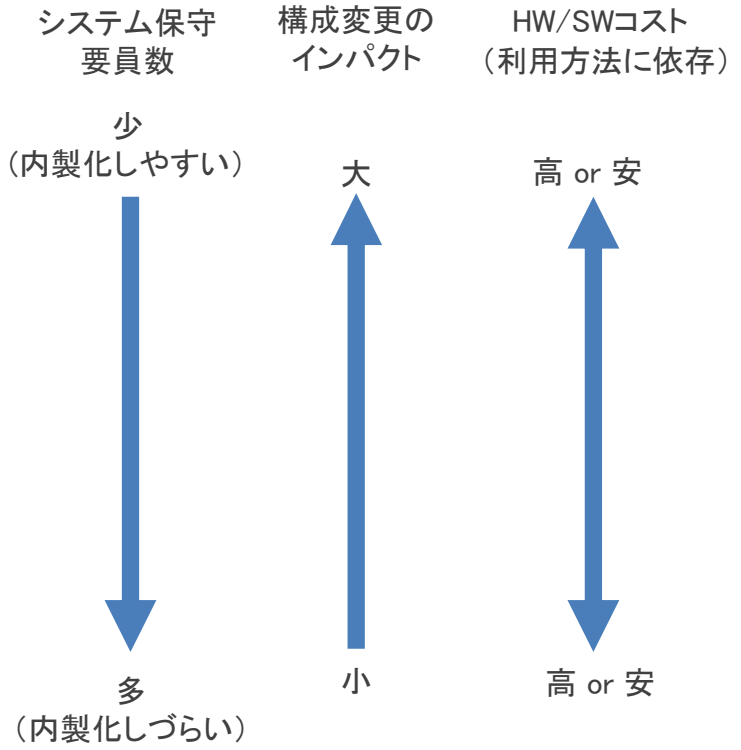
①社内決裁

＜アクション＞

1. 自社インフラ戦略に沿った利用形態かの見極め

自社戦略が、インフラ部門のコア業務(内製化　or　外注化)をどう変えていくのか
全て内製化するか、外注部分をサービスに変えるか、外部委託(人)するか、
戦略にあうアーキテクチャ、利用形態になっているかを見極める。

- A) フルマネージド:サービス化(サーバレス、SaaS)
- B) 部分的マネージド(PaaS、コンテナ)
- C) 部分的マネージド(IaaS)
- D) ユーザマネージド(HCI、オンプレ)



7. 新規・更改　:時期・方式・価値の妥当性
シーン④:次世代アーキ・技術導入および、PoC :　アクション

①社内決裁

＜アクション＞

2. 直接的な効果(コスト、品質、納期、セキュリティ)を示す
   - 導入コスト、運用コスト(内部人件費、外部人件費、もの代)の削減効果
   - 手動オペレーションの削減、過去障害の傾向分析による改善
   - サービス化(構築期間、テスト期間の削減)による納期短縮
   - レガシーシステム・技術からの脱却による人材不足の解消、セキュリティリスクの回避

3. 中長期的な効果(他システム、他プロジェクト、他部門、グループ会社への効果)を示す
   - 本取り組みにより、局所的ではなく、広範囲または、今後の別の取り組みに効果が出るなど

4. 全体最適を考えた取り組みであることを示す
   - 基本的に個別最適はNG(社内政治による例外はある)。如何に全体最適、全体効率化に繋がる取り組みであるかを示す必要がある。

5. 人材育成、ノウハウ蓄積への効果があることを示す
   - 自社インフラ戦略、今後の市場動向に則した取り組みであることを示す。

＜人材育成方法＞
- 立ち上げ期間はアウトソーシングし、その期間内に内部要員がスキルを習得してい、内製化を進める。
- 内部要員を外部ベンダーに1，2年修行に出し、スキル・ナレッジを吸収。外部ベンダーも顧客先との関係性を深める。

7. 新規・更改　:時期・方式・価値の妥当性
シーン④:次世代アーキ・技術導入および、PoC :　アクション

①社内決裁

＜アクション＞

7. (PoCの場合)実行フェーズではなく、事前に行う必要性を示す

8. (PoCの場合)やった場合の効果および、やらなかった場合のリスク
   - 実機でしか気づかないことはあるため、案件規模が大きい場合は実施すべき。

9.(PoCの場合)技術検証環境の準備
   - 従量課金環境の利用。パブリッククラウドや、サービスの利用。
   - その他、ベンダから無償でベンダラボや、機器レンタルが可能な場合もある。

2020年度ITインフラ研究会

分科会A　活動報告
- 海外・グループ会社ガバナンス

ITインフラ研究会　分科会A
海外・グループ会社ガバナンスチーム

目次

はじめに　―　本資料および研究の概要

ガバナンスとは何かを解説

そもそもガバナンスとは？なぜ必要なのか？今後も必要なのか？
そういった観点で、特にガバナンス推進担当の方に少しでも役に立つように
ガバナンスの定義、その必要性、求められる背景等を簡単に纏めています。
今後、各企業においては自社組織だけでなく国内外の拠点やグループ会社、ひいては取引先にもセキュリティのガバナンス・マネジメントを求める必要が出てくることが予想されています。ITのリスクマネジメントの一環として、ガバナンス担当・インフラ・セキュリティ関係の方等是非ご一読いただければ幸いです。

昨今話題のテーマを深堀

各社の取り組み状況、クラウドの統制状況、内部不正対策、
セキュリティマネジメントのフレームワークの採択状況等、
アンケートの中からいくつか抜粋し、各社の動向をピックアップ。
また、**ゼロトラストをどう考えていくか**、等も少々考察を入れています。
皆さんどこまで、どうやっているのか？気になっている方は是非ご覧ください。

超忙しい人向け、本資料のサマリー

なぜ海外のガバナンス？

セキュリティガバナンスは今後もますます求められていく傾向に。
特に、今後はますますグループ、海外、取引先への対応もシビアに。
（NIST CSF/SP800-171対応など）
また、やらないと、業界によっては本気で致命的な損害(数百億)も？

アンケート結果より

-日本国内のガバナンスは各社さんそれなりに利いてきている
-海外、グループ会社まで含めてというのは、比較的まだ進んでいない
-フレームワークとしては、やはりISOが人気である
-クラウドの利活用が進む一方で統制はこれからという企業が多い
-内部不正対策についてUEBAはまだ浸透率が低い

課題と展望

慢性的な人手不足　⇒　海外・グループのガバナンスに使えそうなツール紹介
ゼロトラスト・クラウドシフト　⇒　ベストプラクティス紹介や対応方針を検討

目次

本テーマ選定の背景

■海外・グループ会社のセキュリティガバナンス（およびマネジメント）

■JUAS研究会初回でブレインストーミングを行いました。
議論の結果、セキュリティのガバナンスを推進しようとしている企業がいくつかあり、
各社課題を抱えていることから、これをテーマに選定することにしました。

【挙がった課題・疑問】

◆そもそも情報セキュリティガバナンスとは？
◆ガバナンスのスコープはどうすべきか、どうしているのか？
◆グループ・海外に展開するベストプラクティスとは？
◆セキュリティのフレームワークとしては何が良いのか？
◆各社さんどこまでやっているのか？
◆クラウドの展開と歩調を合わせる必要は？
◆費用負担はどうしている？

本テーマ選定の背景

研究方針・テーマ

セキュリティガバナンス・マネジメントについて、各社の取り組み状況を調査する。

テーマ選定の理由

セキュリティの本質はリスクマネジメント。対策は各社違って当たり前。
しかし一方で、定量的な評価が難しく、実装を悩まれる企業さんが多い。
各社の対策状況をまとめ、皆さんの指針検討の手助けになればと思い選定。

海外・グループを対象とした背景

経産省のサイバーセキュリティ経営ガイドライン等でもサプライチェーンセキュリティの重要性は叫ばれていたが、NIST CSFにも2017年に”Supply Chain Risk Management”の項目が追加された。サプライチェーンやグループ会社の管理というものは今後デファクトで求められるようになっていくと思われるため。

注意事項：本資料での用語と想定読者

■以下、注意事項となります。ご承知おきください。

ガバナンスとマネジメント

セキュリティガバナンスとマネジメントを明確に区別していない。
これは、ITインフラ研究会という性質から、マネジメント視点でのガバナンスというよりも、ITインフラ担当者レベルに落とし込んだ場合の悩み事などを中心に扱っているためである。

想定読者

上記のことから、想定読者は実務担当者～マネージャークラスを想定している。ITやコーポレートガバナンスの専任やCXOクラスにはやや適していない内容が多いかと思われる。
アンケート回答者についても、ITインフラ研究会の参加者であるために、回答もマネジメント層によるものではないケースが多いものと思われる。

背景　ー　なぜ海外やグループのガバナンスを？

従来のガバナンスのベストプラクティス？

統括部門としては、標準化・統一化した方がやりやすい。
一方で、国やビジネスユニット業態により法令や要求事項にが異なる場合がある。
本来的に言えば適切なリスクレベルに応じて対策を定めていくことが望ましいが、
一方で粒度を上げれば上げるほど管理部門の手間は増える。

管理部門が幸せになるためには以下のようなやり方が良いと思われる。
1．ベースラインアプローチとしてレベルを定め遵守させる。
2．情報やビジネスの重要度、業界標準があれば追加として検討する。
3．どうしても費用的についてこれない拠点などはSegregateする

境界型セキュリティではこれが通用した。
しかし、クラウド化し、ゼロトラストの時代には？

背景 ― なぜ海外やグループのガバナンスを？

世界的に強まる情報保護規制

米国

- NIST CSF ver 1.1 Supply Chain Risk Management項目が追加
- NIST SP-171対応要求 国防関係の取引先企業にCUI情報の保護を求める
- カリフォルニア消費者プライバシー法施行

欧州

- European CommissionEU Network and Information Security directive (NIS指令)
- GDPR施行

ASEAN

- 2013 マレーシア 個人情報保護法
- 2016 フィリピン データプライバシー法
- 2013 シンガポール 個人情報保護法
- 2016 インドネシア EIT通信情報省規制
- 2019 タイ 個人情報保護法 他サイバー関係5法令
- 2019 ベトナム サイバーセキュリティ法

https://www.enisa.europa.eu/topics/nis-directive
https://www.ipa.go.jp/files/000066773.pdf

【参考】NIST CSFとは。サプライチェーンリスクマネジメントって？

NIST Cyber Security Framework 1.1 Components

Function	Category
IDENTIFY (ID)	Asset Management (ID.AM)
	Business Environment (ID.BE)
	Governance (ID.GV)
	Risk Assessment (ID.RA)
	Risk Management Strategy (ID.RM)
	Supply Chain Risk Management (ID.SC)
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC)
	Awareness and Training (PR.AT)
	Data Security (PR.DS)
	Information Protection Processes and Procedures (PR.IP)
	Maintenance (PR.MA)
	Protective Technology (PR.PT)
DETECT (DE)	Anomalies and Events (DE.AE)
	Security Continuous Monitoring (DE.CM)
	Detection Processes (DE.DP)
RESPOND (RS)	Response Planning (RS.RP)
	Communications (RS.CO)
	Analysis (RS.AN)
	Mitigation (RS.MI)
	Improvements (RS.IM)
RECOVER (RC)	Recovery Planning (RC.RP)
	Improvements (RC.IM)
	Communications (RC.CO)

"***Cybersecurity really is a supply chain problem***" that encompasses the telecom carriers that are used by businesses, the hardware and software that supports organizational workflow, and the cloud assets that so many organizations are leveraging today, Richard George, former National Security Agency technical director of information assurance recently said in a speech to cybersecurity professionals.

https://www.nationaldefensemagazine.org/articles/2020/7/2/hackers-putting-global-supply-chain-at-risk

https://threatpost.com/nist-updates-cybersecurity-framework-to-tackle-supply-chain-threats-vulnerability-disclosure-and-more/131534/
https://www.complianceforge.com/reasons-to-buy/nist-cyber-security-framework-csf.html

【参考】NIST CSF及びSP-800 171への対応

■NIST SP 800-171とは

■NIST SP 800-171とは米国政府機関が定めたセキュリティ基準を示すガイドラインです。

政府機関だけでなく**取引企業から情報漏洩を防ぐ**ために、**業務委託先におけるセキュリティ強化**を要求しています

◆ NIST SP 800-171より抜粋、一部編集

“本書の目的は、重要情報が連邦政府以外の情報システム・組織にあるときに、
重要情報の機密性を保護するため、連邦政府機関に推奨されるセキュリティ要件を提供することである。”
“重要情報が処理され、保存され、または連邦政府外のシステムを用いる
連邦政府外の組織に送信されるときには、連邦政府機関と同レベルの保護が必要とされる。”

◆ NIST SP 800-171の日本への影響

日本では、**2019年4月**から防衛省および防衛装備庁においてNIST SP 800-171と同程度の新防衛調達基準の試行導入がスタート。**今後は、重要インフラやその他産業への浸透が予想**される。
CUI を扱うために必須となるNIST SP 800-171へ各組織でどのように対応するかが課題。

【対応ステップ】

1.自組織が扱うCUIを定義
2.各要求項目と自組織の現状とのギャップを把握
3.必要な施策を立案して実装する

実装には最低でも1年以上必要。**経営層にてビジネス戦略や経営リスクの枠組に組み込む必要**がある。

https://www.manageengine.jp/solutions/nist_publications/nist_SP800-171/lp/

【参考】金銭的被害額の増加

■データ侵害の被害額は、深刻化しつつある

ここ数年の事例で大きなものは以下のようなものが記憶に久しい。

データ侵害時の費用については、IBMやVerizon、その他保険会社などの試算レポートなども参考になる。

◆ Equifax（約750億円）

米信用情報会社のEquifaxは米国時間7月22日、2017年に起こしたデータ漏えい事件に関する米連邦取引委員会（FTC）や米消費者金融保護局（CFPB）、州当局らによる調査で最大7億ドル（約756億円）を支払うことに同意した。
https://japan.zdnet.com/article/35140265/

◆ マリオット（約130億円）

Marriott Faces $123 Million Fine For 2018 Mega-Breach
U.S. hotel group Marriott has become the second firm to face a massive GDPR fine as the U.K. regulator continues on its rampage. The hotel group, which suffered a breach last year, could face a fine of over £99 million ($123 million). It shows the global impact of the regulation, which covers the personal data of EU citizens.
https://www.forbes.com/sites/kateoflahertyuk/2019/07/09/marriott-faces-gdpr-fine-of-123-million/?sh=45a400ba4525

◆ British Airways（約250億円）

British Airways faces record £183m fine for data breach
The ICO said the incident took place after users of British Airways' website were diverted to a fraudulent site. Through this false site, details of about 500,000 customers were harvested by the attackers, the ICO said.
https://www.bbc.com/news/business-48905907

目次

はじめに：セキュリティガバナンスの定義とは

ガバナンスの定義

セキュリティガバナンスには、いくつか定義が存在している。

- Corporate/IT Governanceと同列にあるものという見方が多い模様。
- Security Managementよりは上位に位置づけらることが多い
- 明確にセキュリティガバナンスとマネジメントを分けるべきであるという論調も。
- 一方リスクマネジメントの一環として、より広義な記述も

(※ただしこの辺りは明確に使い分けをしている企業は多くないという印象である)

ガバナンス・マネジメントのフレームワーク

◆**ガバナンス**としては、
ISOシリーズであればISO 27014、ISO 38500、ISO31000
その他、経産省による定義や、COSO-ERM等が参考になるかと思われる。
◆**セキュリティマネジメント**としては、
ISO 27kシリーズ、NIST、CIS、その他業界標準（例：PCI DSS等）がある。

経産省　サイバーセキュリティ経営ガイドライン も必読

■サイバーセキュリティ経営ガイドラインとは？

➢経済産業省とIPAが共同で策定した**企業向けのセキュリティガイドライン**。
➢企業のセキュリティ対策実施の**指針**。法的強制力はなく、**推奨事項**をまとめたもの。
➢ 経営者を対象として、**サイバー攻撃から企業を守る**観点で、以下をまとめたもの。
- **「３原則」** ― 経営者が認識する必要がある原則事項
- **「重要１０項目」** ― 経営者が担当幹部（CISO等）に指示すべき事項

■海外・グループ会社（及びサプライチェーン）への言及

◆ 3原則の(2)

自社は勿論のこと、ビジネスパートナーや委託先も含めた**サプライチェーンに対するセキュリティ対策**が必要
（自社のサイバーセキュリティ対策にとどまらず、サプライチェーンのビジネスパートナーや委託先も含めた総合的なサイバーセキュリティ対策を実施すべきである。）

◆ 重要事項の指示９

ビジネスパートナーや委託先等を含めた**サプライチェーン全体の対策及び状況把握キュリティ対策**が必要
監査の実施や対策状況の把握を含むサイバーセキュリティ対策のPDCA について、系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先等を含めた運用をさせる。
システム管理等の委託について、自組織で対応する部分と外部に委託する部分で適切な切り分けをさせる。

NRI Secure - 今さら聞けない！【解説】サイバーセキュリティ経営ガイドラインVer2.0
https://www.nri-secure.co.jp/blog/cybersecurity-management-guidelines-2.0

経済産業省 - サイバーセキュリティ経営ガイドライン
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

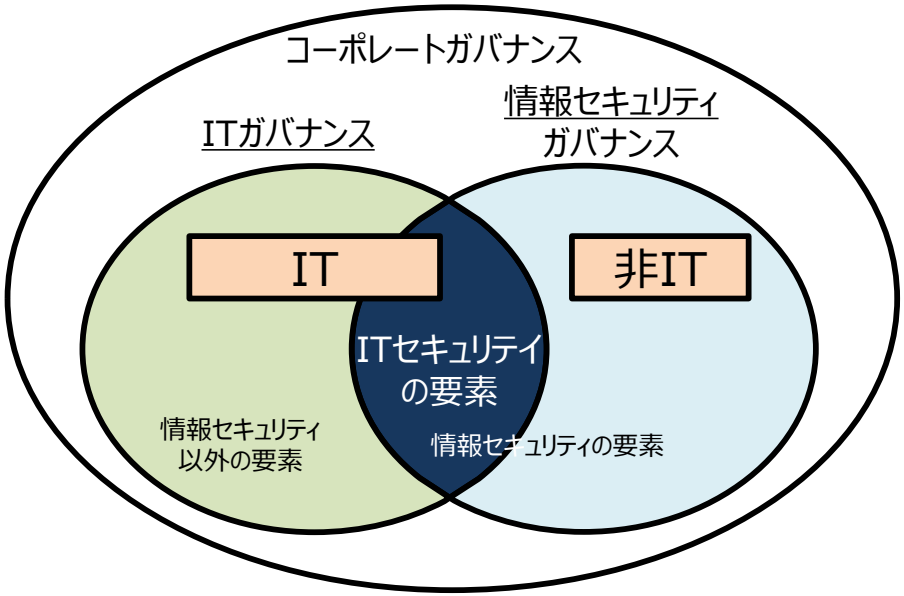
情報セキュリティガバナンスの定義

■情報セキュリティガバナンスとは

「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」(出典：経済産業省ウェブサイト　)において、
「社会的責任にも配慮したコーポレートガバナンスと、
それを支えるメカニズムである**内部統制の仕組みを、**
情報セキュリティの観点から企業内に構築・運用すること」
と定義されています。

(…)つまり**情報セキュリティガバナンス**は、
コーポレートガバナンスの一環として確立されるものであり、
その仕組みとして内部統制を適用するという位置づけになります。

同じくコーポレートガバナンスの一環として確立されるものとして、
ITガバナンスがあります。ITガバナンスとは、経営戦略に則った
IT戦略の策定、およびITの導入・運用を組織的に管理、統制し、
リスクを最適化するための仕組みです。



(※資料中の図を参考に筆者で再現。)

今さら聞けない！情報セキュリティガバナンスとは？
https://infogov-labo.jp/articles/whats_information_security_governance/

図1-1 コーポレートガバナンス、ITガバナンスと情報セキュリティガバナンスの関係 出典：経済産業省ウェブサイト
https://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_gov_guidelines.pdf

情報セキュリティガバナンスの動向や課題

情報セキュリティガバナンスを構築・運用するにあたり、国際標準として**ISO/IEC27014が2013年4月に発行**されました(現在、改訂審議中)。
国内規格としては2015年7月にJIS Q 27014:2015として制定されています。JIS Q 27014は、情報セキュリティガバナンスについての概念および原則に基づくガイダンスであり、この規格を適用することで、組織が情報セキュリティに関連した活動を評価、指示、モニタ及びコミュニケーションできるようになります。

情報セキュリティガバナンスをなぜ、確立しないといけないのでしょうか。2018年6月、東京証券取引所からコーポレートガバナンス・コードの改訂版が公表されました。それによると、第3章「適切な情報開示と透明性の確保」の基本原則3は次の様な考え方に改訂されています。

“上場会社は、会社の財政状態・経営成績等の財務情報や、経営戦略・経営課題、**リスクやガバナンスに係る情報等の非財務情報について、法令に基づく開示を適切に行うとともに、法令に基づく開示以外の情報提供にも主体的に取り組むべきである**。その際、取締役会は、開示・提供される情報が株主との間で建設的な対話を行う上での基盤となることも踏まえ、そうした情報(とりわけ非財務情報)が、正確で利用者にとって分かりやすく、情報として有用性の高いものとなるようにすべきである”

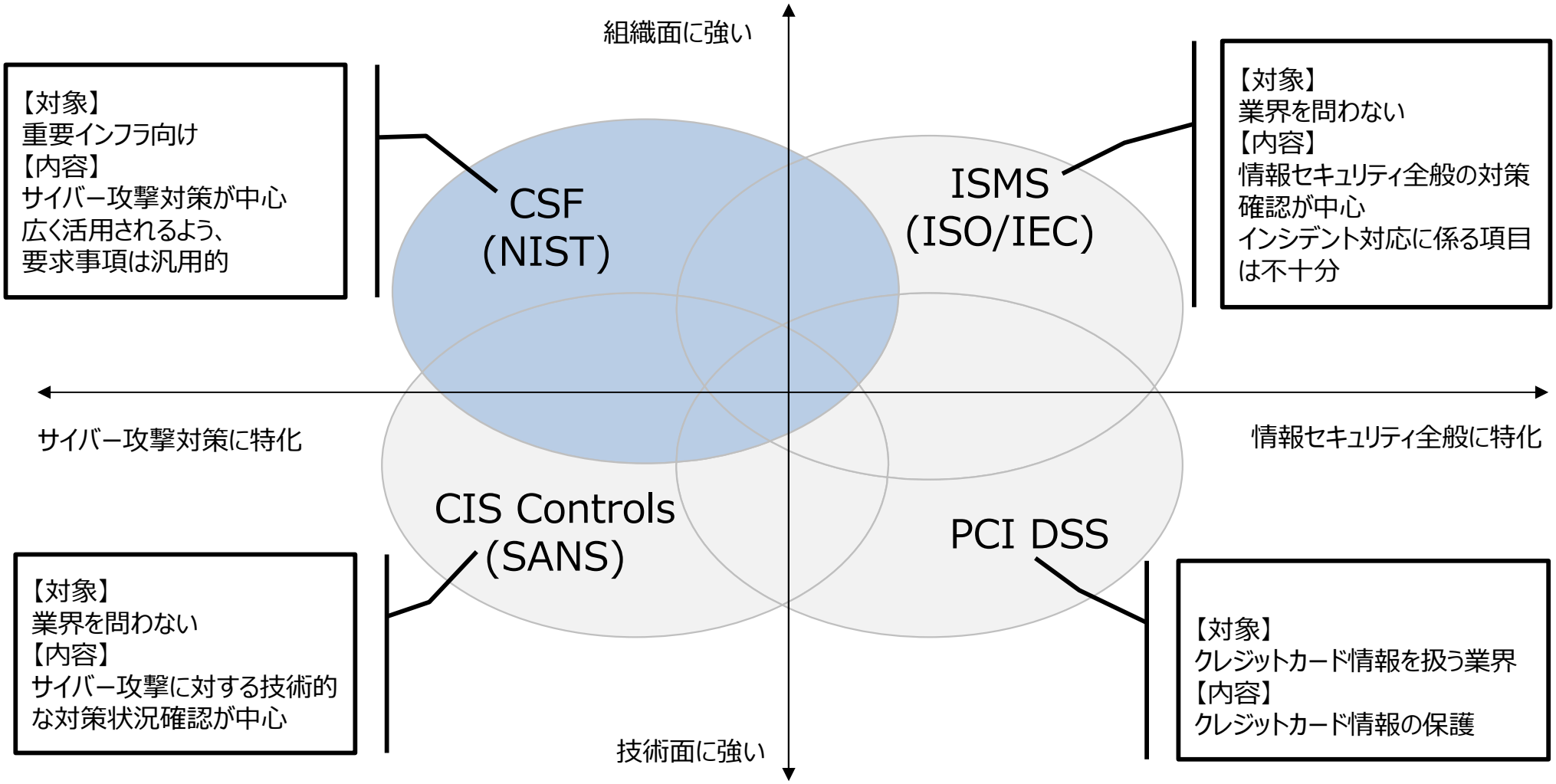
ここで記述されているリスクには、当然、**セキュリティに関するリスクも含まれて**います。
つまり**コーポレートガバナンス報告書に、セキュリティリスクに関しても詳細を記載**することが望ましいと読み取ることができます。

NTTデータや日本電気、富士通、日立製作所、富士ゼロックスなどの大手IT企業を中心に、自社のセキュリティへの取り組みを詳細に記した情報セキュリティ報告書を開示する企業も増えています。情報セキュリティガバナンスを確立する上で、今、**一番の課題となっているのが、SaaSやPaaS、IaaSなどのクラウドサービス**を利用する場合です。
サービスの提供範囲や責任範囲によって、利用者と事業者という形に分かれるので、情報セキュリティガバナンスが複雑化し、確立が難しくなっているからです。また個人や組織でのクラウドサービスやSNSの利用など、「シャドーIT」の問題も情報セキュリティガバナンス確立の障壁となります。この辺りも社員教育をするなどを含め、きちんと整理する必要があるでしょう。

今さら聞けない！情報セキュリティガバナンスとは？
https://infogov-labo.jp/articles/whats_information_security_governance/

【参考】セキュリティマネジメントのフレームワーク

(※資料中の図を参考に筆者で再現。)



NRIセキュア ブログ - 【解説】NIST サイバーセキュリティフレームワークの実践的な使い方
https://www.secure-sketch.com/blog/nist-cybersecurity-framework

目次

アンケートについて

背景

冒頭に示したような課題を抱えるメンバが、
海外拠点のガバナンスを推進する上でのお困りごとを中心にアンケートを編纂した。
その他、各企業でよく聞くような「ありがち」な課題をいくつか追加で質問し、
各社どのような対応をしているのか、対応状況の調査を目的としている。
これより推進を開始する企業や、見直しを行っている企業においては、
本アンケートにより**他社の動向等**を知ることで、少しでも参考なればと思っている。

注意事項

冒頭に記したように、ガバナンスと、マネジメントを明確には区別していない。
海外に拠点がない企業様もあるかと思われたので、あまり対象を絞り過ぎずに、
国内を含めどのようにガバナンスを推進しているのか、という設問にしている。

設問内容(全27問　大きく4セクション)

企業情報全般

Q1: 従業員数
Q2: 業界
Q3: スコープ・体制
Q4: コントロール範囲
Q5: カバー領域

ポリシー・フレームワーク

Q6: ポリシー主管
Q7: モニタリング
Q8: ルールの標準化
Q9: アプローチ手法
Q10: フレームワーク

ポリシー・フレームワーク

Q11: 展開の課題
Q12: 費用負担(コンサル費等)
Q13: 費用負担(ソフト費等)

セキュリティマネジメント・運用・実務

Q14: 独自サービスの利用是非
Q15: CSIRT組織の構築状況
Q16: クラウド利活用統制
Q17: パブリッククラウド統制
Q18: グローバルポリシーの作成
Q19: Q18展開時の課題
Q20: Q19のアプローチ（AS-IS or TO-BE）
Q21: 内部不正対策製品導入状況
Q22: 退職者管理（ID管理）
Q23: 権限管理
Q24: セキュリティ教育
Q25: 教育コンテンツ
Q26: 実務担当者育成（資格取得）
Q27: 実務担当者育成（褒賞）

結果：特筆ポイント

■アンケート結果、特筆ポイント

■特に、世間の最新動向などを念頭に以下の5つのポイントは特筆事項としてフォーカスした。
（※全アンケート結果および、それについての考察はAppendixに。）

サマリー

- ◆ 日本国内のガバナンスはそれなりに聞いてきている
- ◆ 海外、グループ会社まで含めてというのは、比較的まだ進んでいない
- ◆ フレームワークとしては、やはりISOが人気である
- ◆ クラウドの利活用が進む一方で、統制はこれからという企業が多い
- ◆ 内部不正対策についてUEBAはまだ浸透率が低い

※それ以外にも、多数有用な結果が得られているので、
ぜひAppendixのアンケート全結果もご参照ください。

特筆ポイント

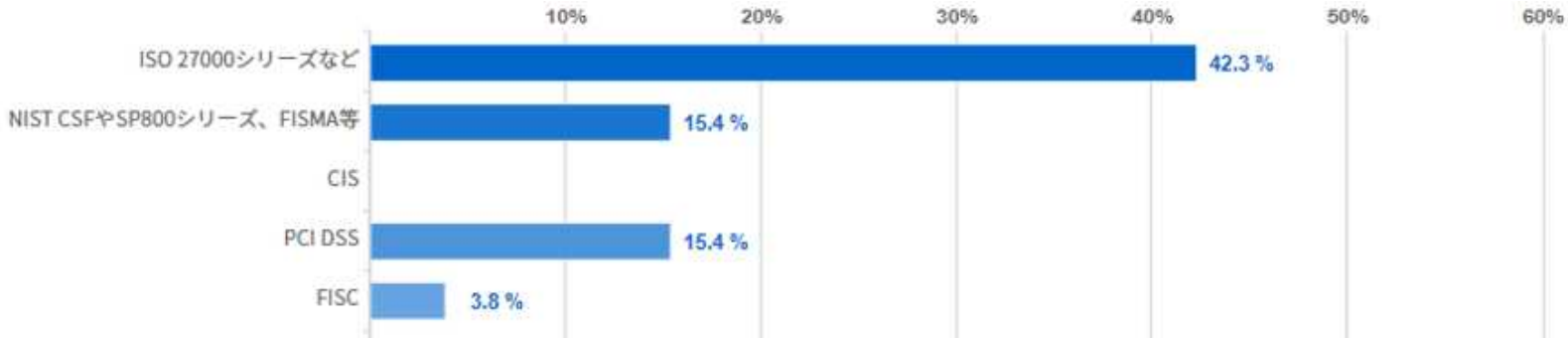
■アンケート結果、特筆ポイント

◆日本国内のガバナンスはそれなりにきいてきている
◆海外、グループ会社まで含めてというのは、比較的まだ進んでいない

【考察】「国内のグループ会社を含め、ある」という回答は50%にのぼっており、国内では半数の企業はガバナンスの体制があることがうかがえた。一方で、海外に関しては子会社・支社・拠点でも26.9%、グループ会社となると19.2%という状況で、国内に比べるとやはりまだ着手中の会社が多いことがうかがえた。**昨今のサプライチェーン上のリスクマネジメントを考慮すると、これらの企業の管理というものも急務である。**

特筆ポイント

◆フレームワークとしては、やはりISOが人気である



【考察】 日本企業では**ISOが人気**というのは聞くが、如実に表れた結果となっている。一方で、NIST CSFやFISMA、PCI DSSについても少数ながら採択している企業があった。どちらの規格が優れているということはないが、冒頭にあるように、**NIST CSF/SP800-171等の対応**があり、今後NISTに基づいた対応が求められるシーンが増えるかと思われる。フレームワークの実装には時間がかかるために、早期より次のような対応を行っていくことが肝要かと思われる：

◆ISO系の規格を採用している場合

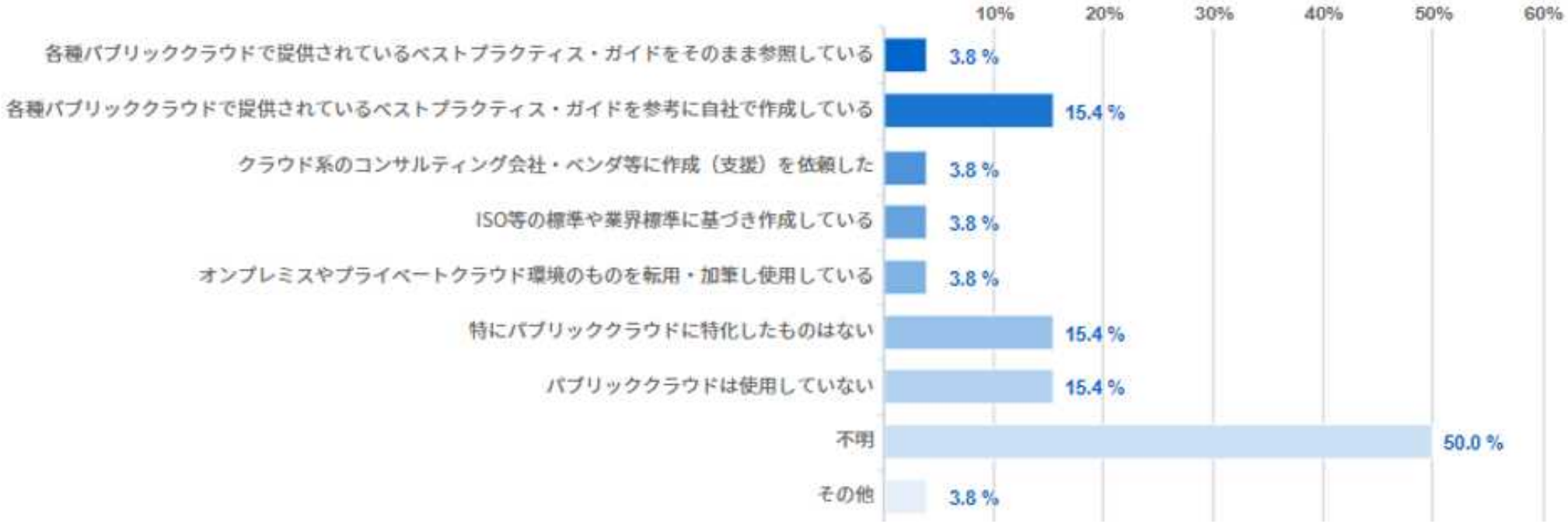
⇒ISOとNIST CSFとの対応関係を整理した上でのFit＆Gap分析を行う。

◆現在認証を取得していない場合

⇒リスク分析を行い、自社・取引先に対して特にクリティカルとなるビジネスプロセスやデータ、システムを洗い出し、NIST/ISO等のフレームワークをベースに、対策を検討する。

特筆ポイント

◆クラウドの利活用が進む一方で、統制はこれからという企業が多い



【考察】 全体として、「不明」が最も多いことに加え、回答状況もマチマチであった。参考までに、**Azure, AWSのようなパブリッククラウドではそれぞれセキュリティのベストプラクティス等を公開**している。そのまま採択することも可能かもしれないが、自社組織にテイラリングして規程を定めるのが良いかと思われる。特に、パブリッククラウドは従来のオンプレミスと比較しセキュリティの設計がそのまま適用できない可能性も高いために、一度リスク分析を行ってみることが良いかと思われる。

【参考】 セキュリティのベストプラクティス

Azure

Azure セキュリティのベスト プラクティスとパターン

https://docs.microsoft.com/ja-jp/azure/security/fundamentals/best-practices-and-patterns

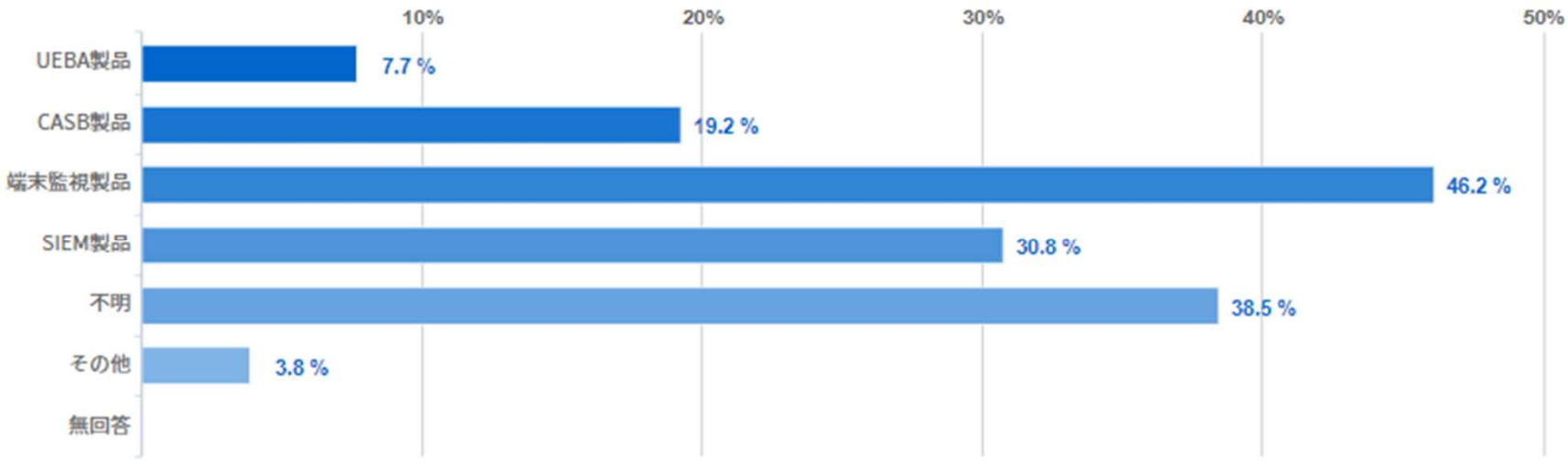
AWS

AWS セキュリティのベストプラクティス

https://d1.awsstatic.com/International/ja_JP/Whitepapers/AWS_Security_Best_Practices.pdf

特筆ポイント

◆内部不正対策についてUEBAはまだ浸透率が低い



【考察】 昨今は、内部不正対策もよく耳にするようになった。Forresterが2018年に公開したZero Trust Extended等の文脈の中でもSIEMやUEBAといった言葉は耳にする機会が増えたように思う。しかしながら、採択状況としては上記の通り、まだ多くないというのが実情であった。現状では端末監視系のソフトが現状では大きな割合を占めている。
とはいえ、SIEMは約3割と、かなり認知度・採用状況が向上してきているということが見受けられる。セキュリティの可視化、分析といった領域は今後も洗練化が進んでいく領域であるだろうと思われるが、**現状は様子見をしている企業が多い**のかと思われる結果となった。

目次

Tips: 海外・グループ・その他多数の管理対象…どう管理していくか？ － ツール紹介

人手は中々つらいです。ツールを利用しよう

可視化し、定量的に継続的にモニタリングを行っていくことが重要。

Garnterピアインサイツより：IT Vendor Risk Management (VRM) Tools
ベンダー評価ツールは多数あり、自社のニーズに応じて利用していくのが良い。

IT Vendor Risk Management (VRM) Tools Reviews and Ratings
https://www.gartner.com/reviews/market/it-vendor-risk-management

Tips: 海外・グループ・その他多数の管理対象…どう管理していくか？ － アプローチ

全体最適的にはグループで統合すべきか？

グループで統合することのメリット
- ・セキュリティ対策状況の把握が容易になる。
- ・ボリュームディスカウントなどがきくようになる。
- ・調達や更新の管理が一元化される。
- ・ログ管理、SIEM取込やMSSとの連携も容易。
- ・脆弱性対応が一元管理できる。

等々・・・多数メリットあり。

課題としては、
- ・費用負担。
- ・事業が違う(セキュリティレベルが違う)
- ・会社により利用しているシステムやクラウド、取り扱っているデータの重要度が違う・・・

等々の問題で、海外拠点は中々難しいことも。

現実的にはアプローチとしては、
- ・セキュリティをCXOからトップダウンで行う。
- ・セキュリティ関連事項を契約次項に盛り込む。
- ・ボリュームディスカウント等でトータルコストの低減を説明

等々。一筋縄でいかない場合が多いが根気強く説得が必要のようだ。

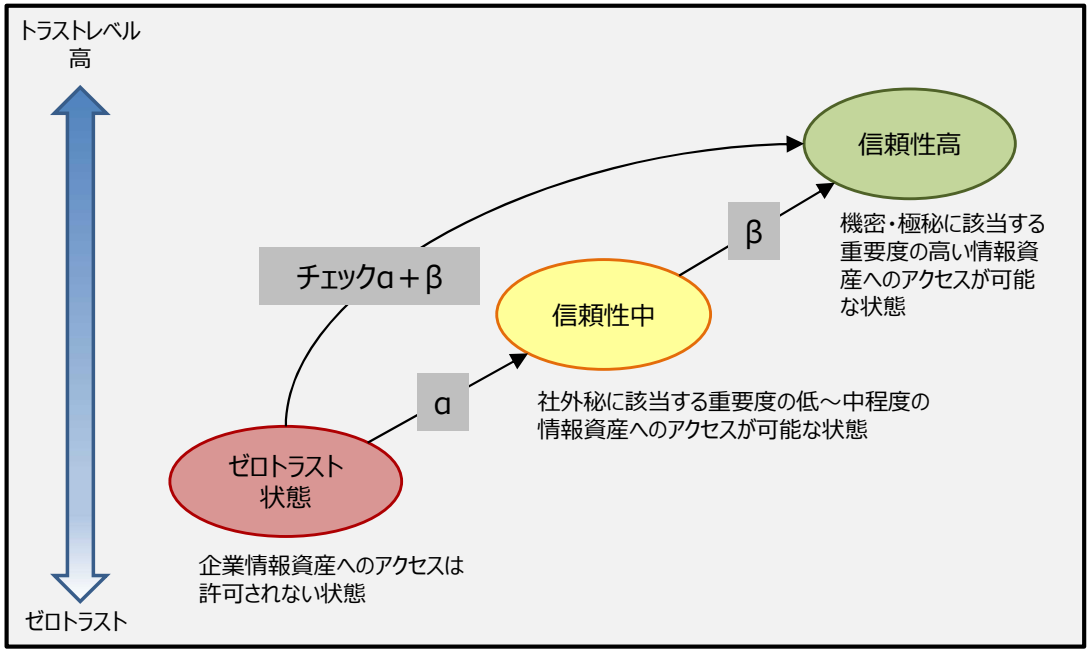
ゼロトラストとどう向き合っていくか？

ゼロトラストはむしろガバナンスには好機

バズワード化しているゼロトラスト。本質的にはアクセス権の見直しであるといえる。
例えば、これまでグレーゾーンであった、ベンダーさんや、海外子会社、取引先、等々
アクセス権やセキュリティの見直し及び統一化を進めるうえでいい切り口となりえる。

IBMセキュリティー・インテリジェンス・ブログより

(※資料中の図を参考に筆者で再現。)



“重要となるのは、トラスト状態に遷移する際に行うチェックをどの程度まで実施するかです。
（中略）トラスト状態のリスクレベルは、企業が持つ**情報資産の重要度やセキュリティーにかけるコストの大きさ、リスクの許容度に依存**するため、
ゼロトラスト・セキュリティーを導入しようとする企業は、**リスク評価に基づいたセキュリティー設計**を行うことが求められます。“

⇒結局BIA/Risk Assessmentが重要

- どこに重要資産があるのか？
- 誰がどういう状況ならばアクセスさせてよいのか？

このポリシー設計と、ポリシーのエンフォーサ（どのレイヤーで、どのように実装するのか）をしっかり検討しないと文字通り“ゼロトラスト“状態になってしまいます。

IBM -ゼロトラスト・セキュリティーの要諦
https://www.ibm.com/blogs/security/jp-ja/what-is-zero-trust-security-what-is-needed/

※なお、エンフォーサは、現在は主にIAP (Identity Aware Proxy)等の、プロキシや、L7のLBを用いられていることが多いように思います。

【補足】ゼロトラストのおさらい① その歴史

もはや昨今は宣伝文句・商材となってしまったゼロトラスト。いったんちょっと、振り返りをしましょう。

2007
- Jericho Forum 「トラストモデル」の提案。
- ホストの防御力向上で境界防御不要を目指す考え。

恐らく初の“De-perimeterisation”の考え方。
一説にはこの言葉は、Jon Meashamが起源とされている。

2010
- おなじみ(?)、John Kindervagによるゼロトラストモデルが提唱される。

2017
- Evan Gilman, Doug Barth （2017)らにより以下書籍発行
- Zero Trust Networks: Building Secure Systems in Untrusted Networks

広く一般に考え方が伝わったのはこの書籍が初めてか？

2018-19
- Forrester Zerotrust Extendにて7要件を定義
- 19年「Zero Trust eXtended Ecosystem Platform Providers」調査結果発表

2019-20
- NISTより19年9月SP 800-207: Zero Trust Architecture (ZTA) Draft 1が発行
- 20年2月にDraft 2が発行
- 必ずしも全面的にZeroTrsut化しない、Hybrid Zero Trustという考え方が提唱

具体的な構成要素が発表されたことで、各社が特に商材として扱い始める。認知度が高まってきたのはこのあたりか？

【補足】ゼロトラストにまつわる誤解と推奨

よくある誤解・間違い

ゼロ トラストという言葉を文字どおり受け取る: 環境内で絶対に何も信頼しないというのは、現実的でないですし可能でもありません。セキュリティ投資を考える際に、コンポーネントに障害が発生する可能性はもちろんありますし、時間とリソースにも制限があります。言葉の意味が文字どおり絶対的であるという考え方は、賢明な判断の助けにはなりません。

ゼロ トラストになろうとする: 貴社がゼロ トラストの状態に「なる」ということはありません。製品がゼロ トラストに「なる」こともできません。ゼロ トラストは、資産を保護するためのアプローチです。これは、戦略と投資の指針となる考え方です。

ゼロ トラストはお金で買える: 製品を購入してインストールし、ゼロ トラストに「なる」ことはできません (マイクロソフト製品でも無理です！)。リスクが蔓延している世界で、1 つの見方や 1 つのアプローチ、1 つの製品を完全に信頼することは、直感に反しています。

ゼロ トラストですぐに解決する: 環境内の前提を変えていくには時間がかかります。一番盲点になっている場所から優先順位を付けていきましょう。散らかった部屋を掃除するように、ある面から始めて、うまくいったらまた先に進むように、まずは一つ取り掛かる場所を決めましょう。

ゼロ トラストがゴールである: 今あなたが身に着けようとしているのは、自身が持つ前提に継続的に疑問を投げかけ、監視データと実際の違いに目を向け、現在のセキュリティ体制を根本的に疑いつづけるという考え方です。この考え方が身につけば、次はどこにどうセキュリティ投資をしていくかという方向にあなたのキャリアが向かっていくでしょう。

ゼロ トラストはすべての企業規模に適用可能である: 組織にとって適切な投資は、現在のビジネス状況がどうか、何を守りたいのか、社員がどう働くのか、インフラ投資戦略はどのようなものかの組み合わせに依存します。ゼロ トラストへのアプローチも、貴社の現在の状態と知見の組み合わせで異なります。

ゼロ トラストは革命である: ゼロ トラストの概念につながる変化の歴史でお話したように、サイバー セキュリティ モデル (例えば “多層防御”) は何十年も進化しています。貴社が採用したものの多くは必要ですが、おそらく十分ではありません。使えるものは使ったほうがいいですが、その制約の中で貴社環境に思い込みや前提ができてしまうようなことは避けなければいけません。

ゼロトラストの考え方

これで完璧だと思い込まない: これはゼロ トラストの最大の変化です。小規模なネットワークと VPN の世界であれば、リクエストが既知のネットワークから発信されている場合、それは通常安全です。私たちは、昨日私たちを守ってきたモデルが明日も私たちを守ってくれると思いがちです。ゼロ トラストでは、これらの思い込みを放棄し、代わりにアクセスの可能な限り多くの側面を検証および制御します。また、実施可能な検証を明示化し、明示的に検証していないものは、不明な状態にあるということも受け入れます。

すべてのリソースがオープンなインターネット上にあると想定する: 凝り固まった思い込みに対応するために、多くの顧客で有効だったアプローチの 1 つは、すべてのユーザー、デバイス、およびリソースがパブリックなインターネット上にあると想定することです。最も成功しているお客様の多くは、この考えにのっとり、できる限りのリソースをクラウドに移動し、セキュリティ戦略を最新の状態にしています。

単一のソースを信頼しない: 脅威が蔓延した環境では、正確な知見が重要です。とある CISO (最高情報セキュリティ責任者) は以前に、「親父が言ってたのは、正直な人は皆同じ話をするが、嘘つきは全員違う話をする」と話してくれました。複数の情報を検証して利用するセキュリティ モデルは非常に強力です。一つの視点から検証するよりも、三点から検証するほうがはるかに正確な情報が得られます。同様に、複数の要素 (デバイスの信頼、場所、多要素認証) を活用した制御のほうが、アクセスの 1 つの側面のみを使用した制御よりも優れています。

侵害の封じ込め: 脅威が蔓延している状況を想定する場合、一部の脅威が防御を突破してしまうことも考えられます。特権 ID 管理やロールベースのアクセス、役割の分離やネットワークのセグメント化などの封じ込め戦略は、防御の最初のレイヤーを突破する敵を封じ込めるのに有効です。

標準技術はセキュリティ: 革新は素晴らしいものの、セキュリティ (特に暗号化) では、数学的に証明できないものは安全ではないという格言もあります。ただ、侵害されるまでにどれだけ時間がかかるかというのは良い指標になります。”実際のセキュリティ向上にはつながらないが見た目から安心感を得ること (Security Theater)” や “システムの仕様を非公開にすることによって安全だとみなす (Security through obsecurity)” ことはやめましょう。厳重に検査され、頻繁に使用され、厳しく攻撃にさらされた標準技術は、セキュリティ戦略の優れた基盤となります。OAuth 2.0 などの最新の認証標準、SCIM などのプロビジョニング標準、および FIDO2 などの資格情報の標準を可能な限り活用しましょう (または、対象の製品を購入しましょう)。

人手はいくらあっても足りません: 可能な限りすべてを自動化しましょう。恐らく大量の監視データと攻撃にあうと思いますが、それらを処理するのに十分な人員は確保できません。クラウドの知能、機械学習を活用し、さらに危険なアカウントを自動的にロックしたり、既知の不正な IP アドレスからのトラフィックを禁止するような自動応答メカニズムを使用することも非常に重要です。

Japan Azure Identity Support Blog
https://jpazureid.github.io/blog/azure-active-directory/zero-hype/ より

【補足】ゼロトラストの原則

- 思い込みや決めつけをやめて、明示的に検証するようにします。
- ポリシー ベースの最小特権アクセスモデルを採用します。
- システムのすべての要素は侵害される可能性があるという前提で設計します。

Japan Azure Identity Support Blog
https://jpazureid.github.io/blog/azure-active-directory/zero-hype/ より

どのように設計するのか？

- NIST, Microsoft, Googleの概念図を参考になる。
  具体的な実装はそれぞれ若干異なっているが、
  - IdentityとDevice(System, Context)を必ず検証している。
  - アクセス制御を司るPolicyのEnforcerが中核にある。

【補足】ゼロトラストのおさらい① NISTの概念図

NIST SP 800-207
3 Logical Components of Zero Trust Architecture より

(※資料中の図を参考に筆者で再現。)

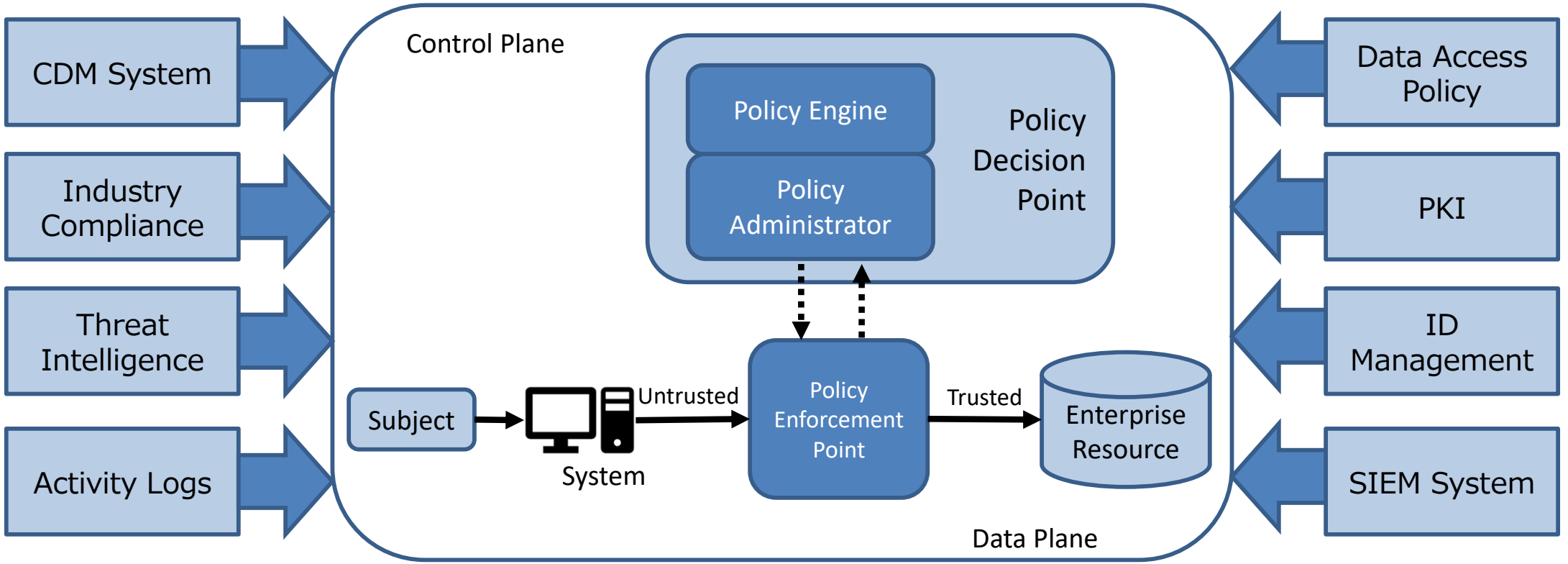


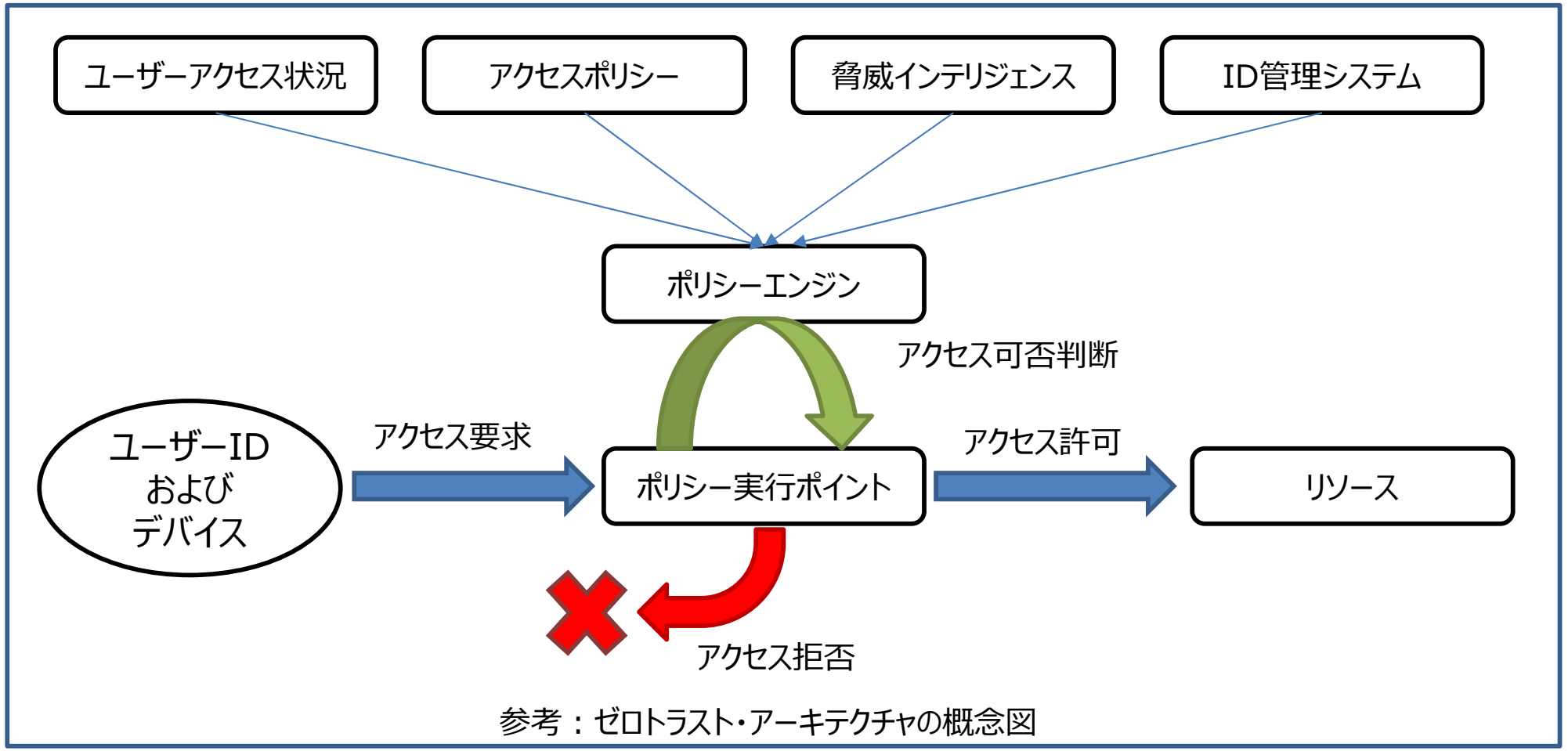
Figure 2: Core Zero Trust Logical Componentsより

NIST Special Publication 800-207
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

【補足】ゼロトラストのおさらい①　政府CIOポータルより

政府情報システムにおけるゼロトラスト適用に向けた考え方より

(※資料中の図を参考に筆者で再現。)



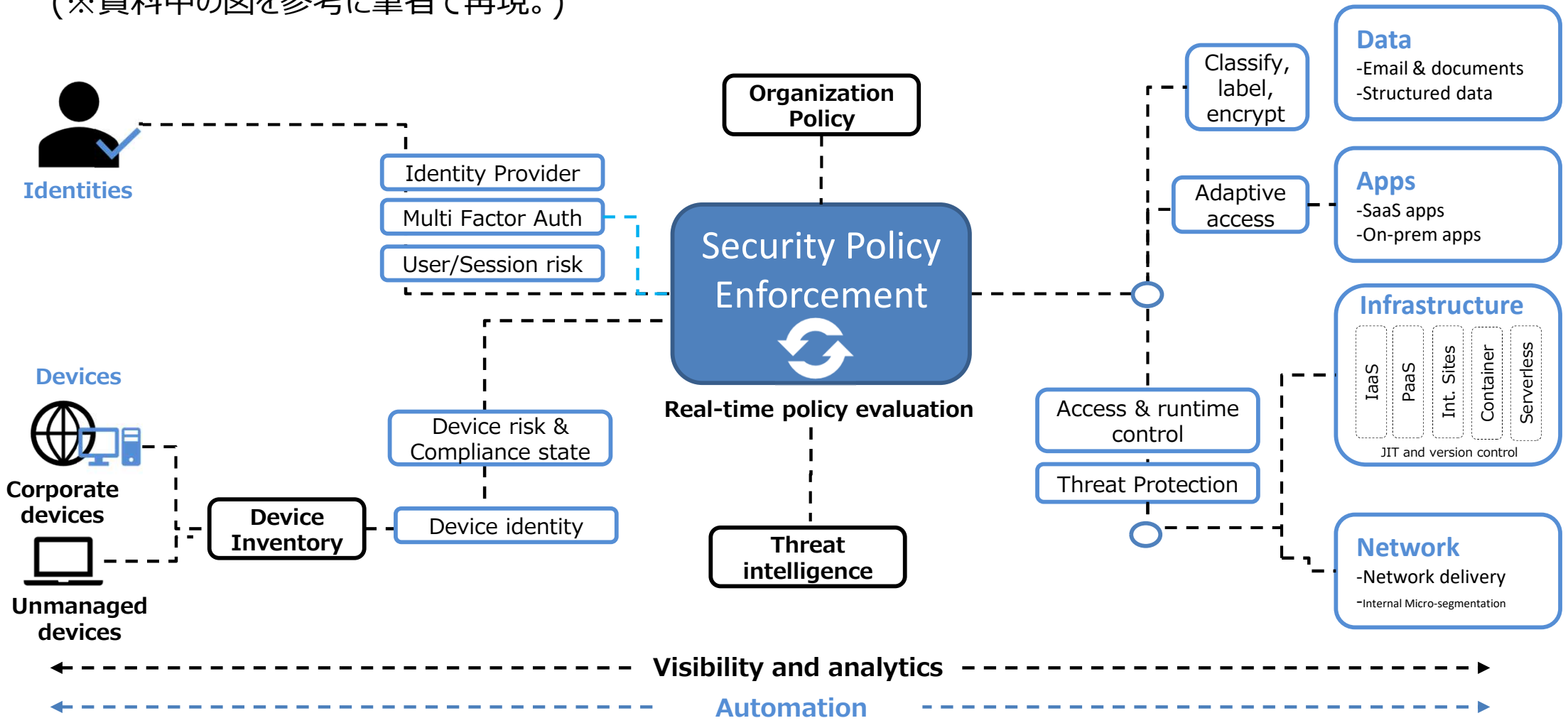
参考：ゼロトラスト・アーキテクチャの概念図

政府情報システムにおけるゼロトラスト適用に向けた考え方
https://cio.go.jp/sites/default/files/uploads/documents/dp2020_03.pdf

【補足】ゼロトラストのおさらい① Micsrosoftの概念図

Microsoft Enable a remote workforce by embracing Zero Trust security より

(※資料中の図を参考に筆者で再現。)



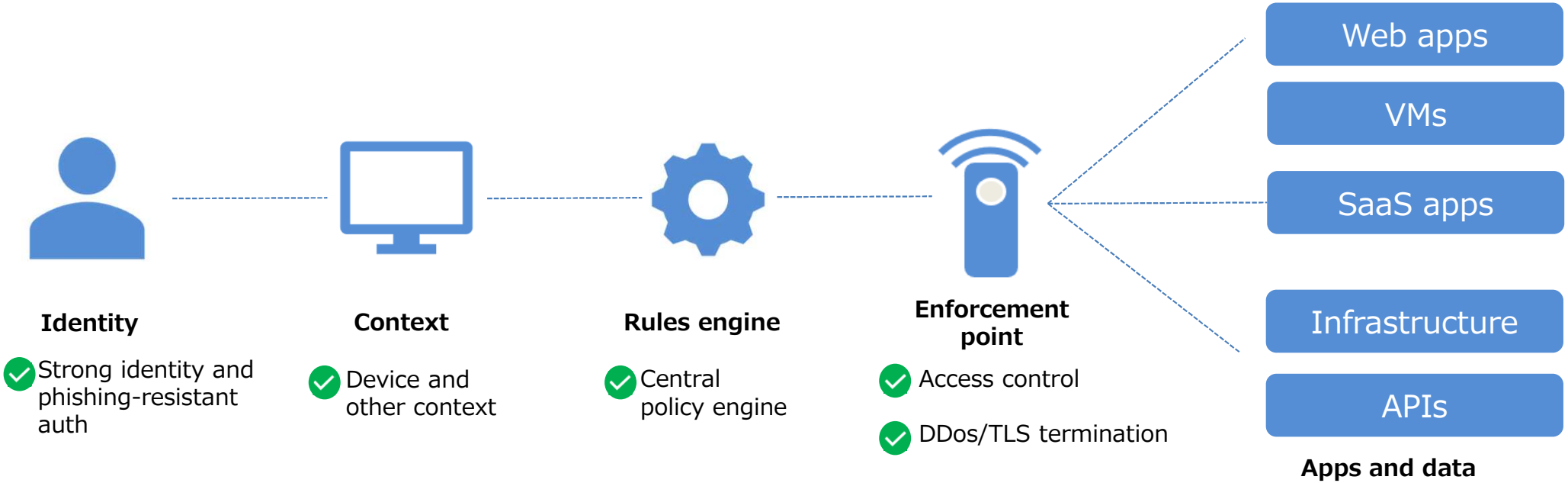
Enable a remote workforce by embracing Zero Trust security
https://www.microsoft.com/en-us/security/business/zero-trust より

Japan Azure Identity Support Blog
https://jpazureid.github.io/blog/azure-active-directory/zero-hype/ より

【補足】ゼロトラストのおさらい① Googleの概念図

Google Security Blog How Google adopted BeyondCorp より

(※資料中の図を参考に筆者で再現。)



High level architecture for BeyondCorp

Google Security Blog - How Google adopted BeyondCorp
https://security.googleblog.com/2019/06/how-google-adopted-beyondcorp.html より

【補足】ゼロトラストの原則

【再掲】

- 思い込みや決めつけをやめて、明示的に検証するようにします。
- ポリシー ベースの最小特権アクセスモデルを採用します。
- システムのすべての要素は侵害される可能性があるという前提で設計します。

データセキュリティ(アクセス権の設定)には昔から、以下の二原則があります。
“Least Privilege“ – 必要最小限のデータのみにアクセスさせる。
”Need to know” – 業務やタスクを行う上で必要性を確認する。

ゼロトラストは、本質的にはこれらを細かい粒度で継続的に行えるようになる考え方といえるでしょうし、そうあるべきです。
なんだかんだで、ゼロトラストへシフトする際には、情報資産の特定・アクセスポリシーの見直し・リスク評価のためにユーザがアクセスするデバイス/システム/コンテキストの特定等が肝要と思われます。これは、ISMS等をやっている人たちから見ると、非常に当たり前のことに思えるでしょう。

また、逆説的かもしれませんが、標準端末・標準デバイス(コンテキスト)は定義しておいた方が運用上のリスク管理は楽でしょう。いつでもどんな端末から・・・というのは理想的ですが、その場合、イレギュラーが発生するたびにリスクを許容するか、リスクの再評価を行う必要が出てくるでしょう。

目次

まとめ（再掲）冒頭と同じです。
ここまでお読みいただき、ありがとうございました。

なぜ海外のガバナンス？

セキュリティガバナンスは今後もますます求められていく傾向に。
特に、今後はますますグループ、海外、取引先への対応もシビアに。
（NIST CSF/SP800-171対応など）
また、やらないと、業界によっては本気で致命的な損害(数百億)も？

アンケート結果より

-日本国内のガバナンスは各社さんそれなりに利いてきている
-海外、グループ会社まで含めてというのは、比較的まだ進んでいない
-フレームワークとしては、やはりISOが人気である
-クラウドの利活用が進む一方で統制はこれからという企業が多い
-内部不正対策についてUEBAはまだ浸透率が低い

課題と展望

慢性的な人手不足　⇒　海外・グループのガバナンスに使えそうなツール紹介
ゼロトラスト・クラウドシフト　⇒　ベストプラクティス紹介や対応方針を検討

謝辞：ありがとうございました。

お読みいただき、ありがとうございました。

次項よりAppendixとして、
アンケート結果を各設問毎に紹介します。

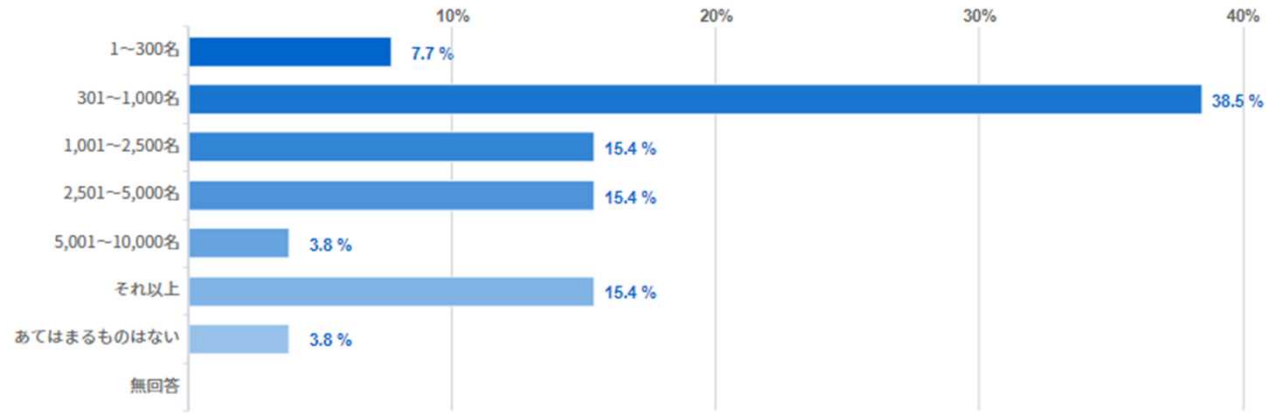
2020年度　ITインフラ研究会
分科会A：海外・グループ会社ガバナンス研究チーム

「海外・グループ会社のセキュリティガバナンス」
Appendix: アンケート結果掲載

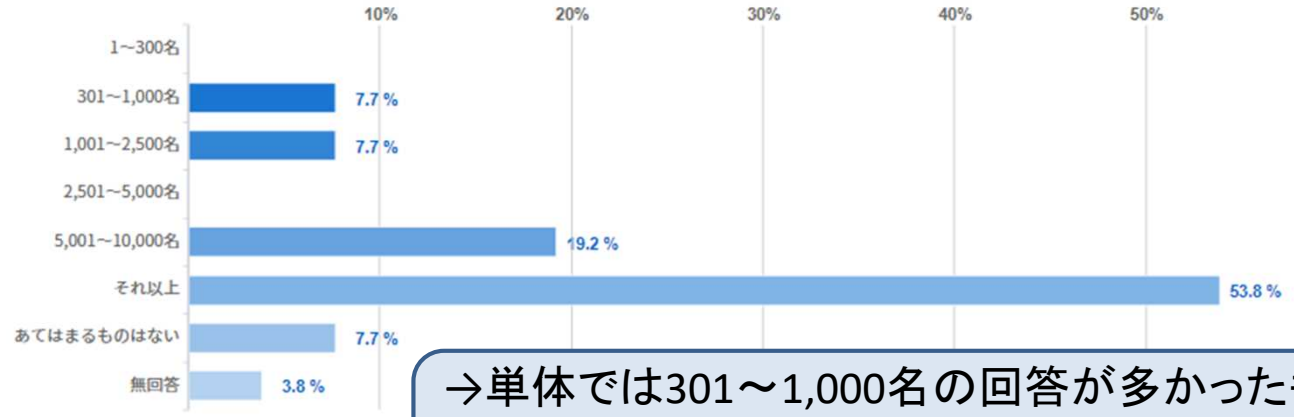
Aチーム

Q1. はじめに、差し支えなければ概ねの従業員数を教えてください。（可能であれば単体・連結それぞれ）

単体
(回答数: 26)

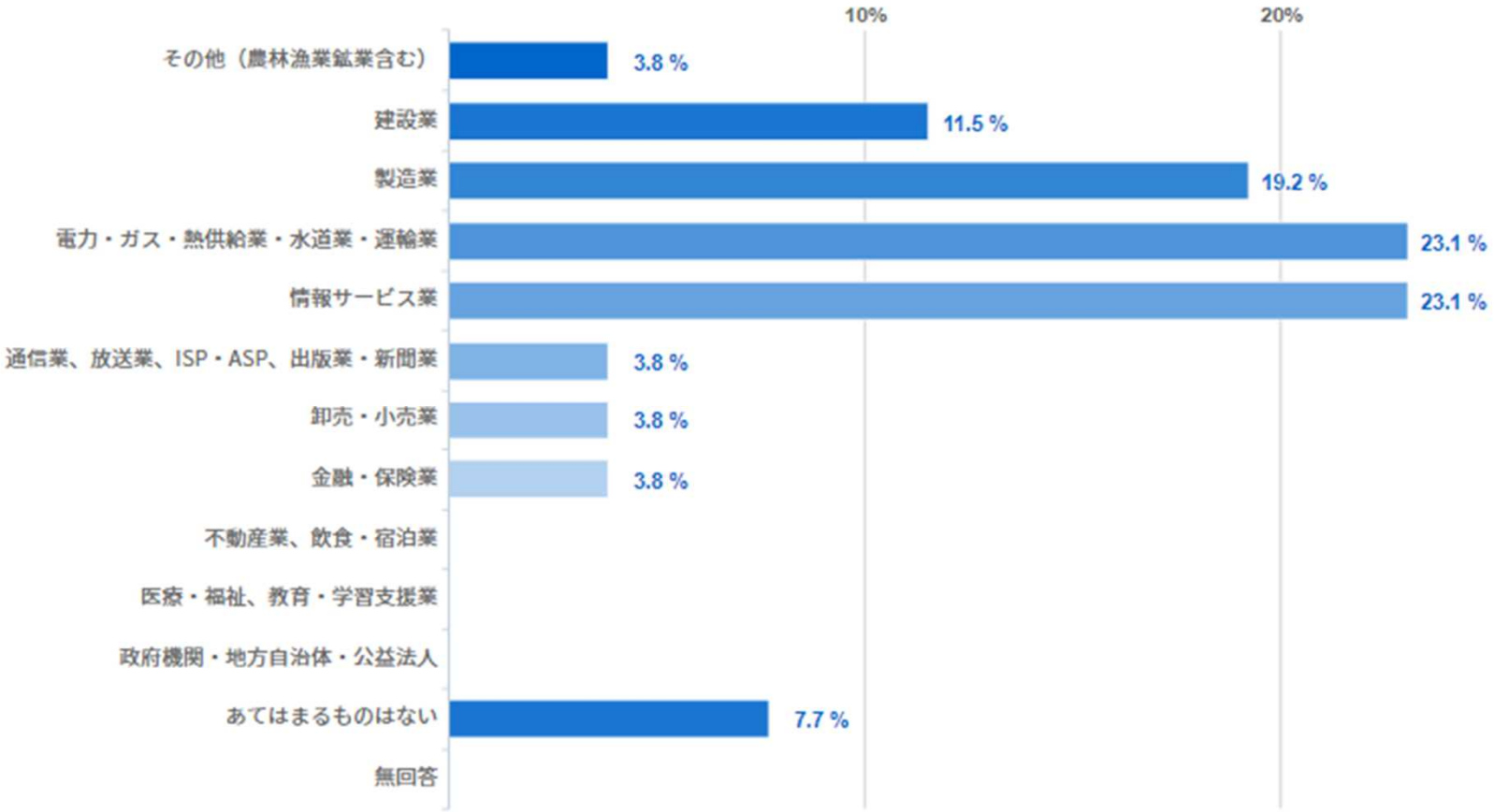


連結
(回答数: 26)



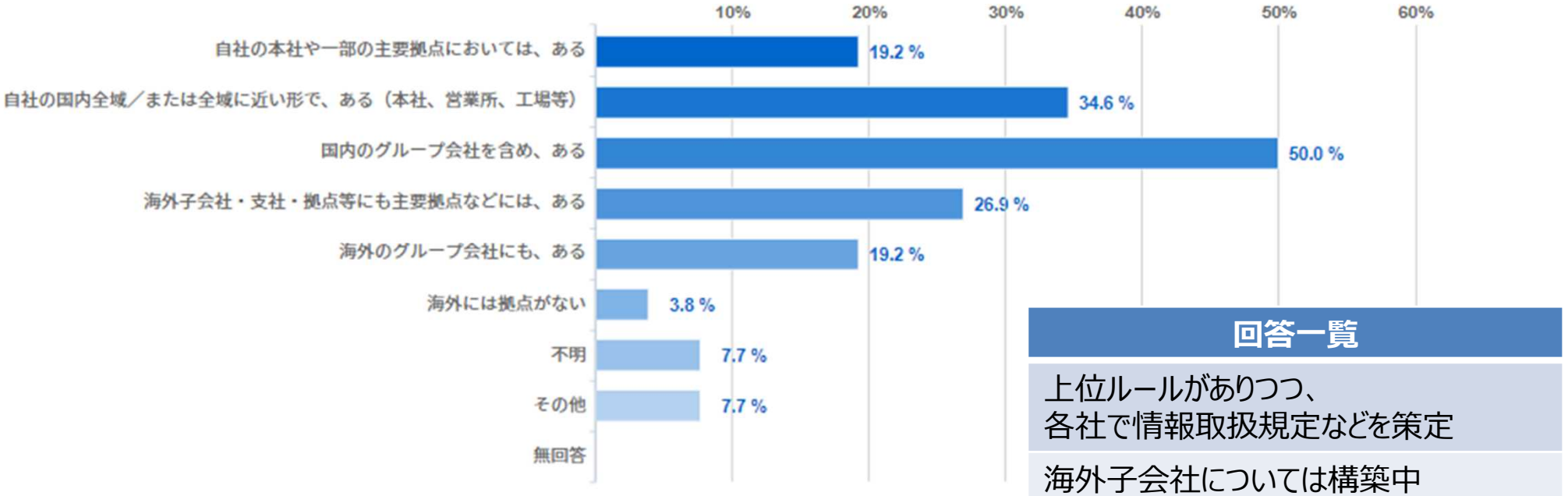
→単体では301～1,000名の回答が多かったものの、連結では1万以上という回答が多く、特に大規模なグループを有している企業の動向を伺う上で良い集計になっているかと思われる。

Q2. はじめに、貴社の所属する業界を教えてください。



→電力・ガス・熱供給業・水道業・運輸業および、情報サービス業はやや多いものの、そこまで極端な偏りはなく様々な業界の回答が収集できた。

Q.3 海外拠点やグループ会社問わず、情報セキュリティのガバナンスについて明確なスコープやゴール、体制がありますか。



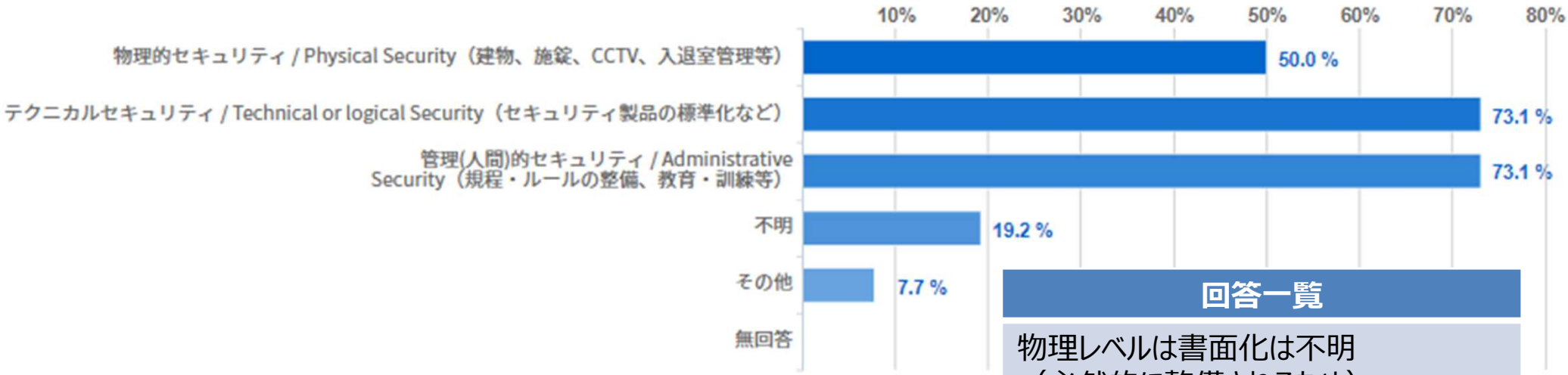
回答一覧

上位ルールがありつつ、
各社で情報取扱規定などを策定

海外子会社については構築中

→国内であれば、グループ会社含めガバナンスを行っている割合が50%と高い割合であった。一方で海外子会社やグループ会社は、決して低くないものの、国内と比較しやや手が回っていないか、海外は管理外、という回答内容になっている。

Q4. 海外拠点やグループ会社問わず、情報セキュリティのガバナンスを行っている場合、現在対象としている領域は主にどのようなところですか。



回答一覧

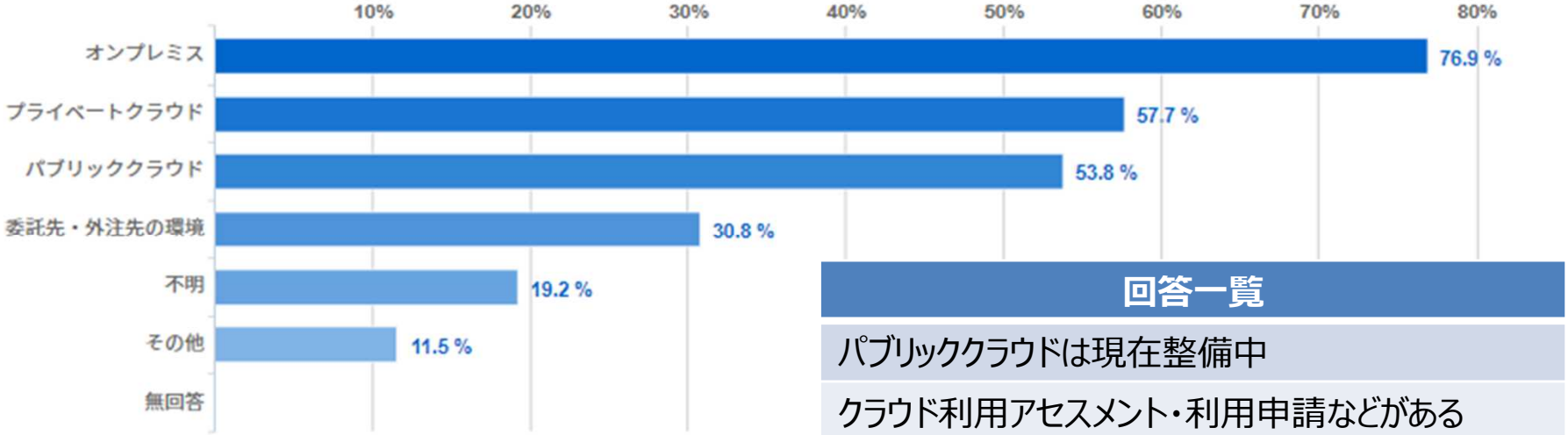
物理レベルは書面化は不明
（必然的に整備されるため）

テクニカルについてはポリシーを策定中

→セキュリティコントロールの三大要素は、いずれも過半数がカバーされていた。一方で、物理的セキュリティは他二つに比べるとカバレッジが若干薄い。IT/セキュリティのガバナンスとは毛色が異なるために、例えば所管が総務部等でITとは区分けされていると、いった企業が多いのかもしれない。

一般的に、物理的セキュリティティというのはその他のセキュリティを設計するうえでの前提となるものであり、これをベースにセキュリティルールを設定している場合が多いかと思われる。しかし今後、ゼロトラスト化が進む場合、その考え方を見直す必要が出てくるかもしれない。Hybrid ZeroTrust環境においては特に物理的セキュリティが確保されている場合とされていない場合でのリスクレベルの再評価が必要となるだろう。

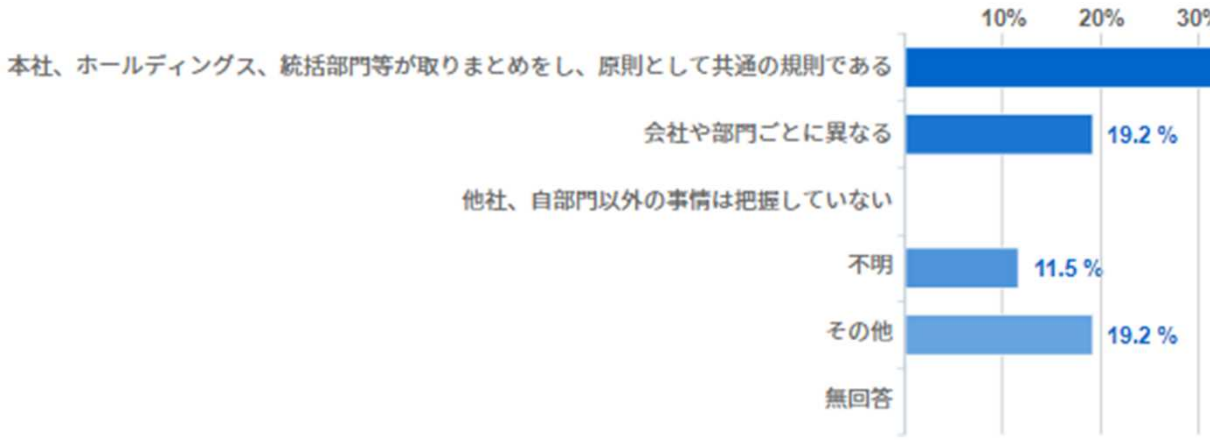
Q5. 海外拠点やグループ会社問わず、情報セキュリティのガバナンスについて現在カバーしている領域はどこになりますか。



回答一覧
パブリッククラウドは現在整備中
クラウド利用アセスメント・利用申請などがある
紙などで保管している文書やUSBなどのOA機器

→大多数の企業ではオンプレミスが主眼であることがうかがえる。しかし一方で、パブリッククラウドでも過半数を超えており、多くの企業でパブリッククラウドの利活用が進んでおり、そのマネジメント・ガバナンスも行っていることがうかがえた。
サプライチェーン上のセキュリティマネジメントの重要性が叫ばれているが、委託先、外注先の管理に踏み出している企業も30%を超えており、こちらも今後数値が増えていくことが予想される。
この先もXaaS等の利用が増えることでガバナンスの対応範囲も変わってくることが予想される。

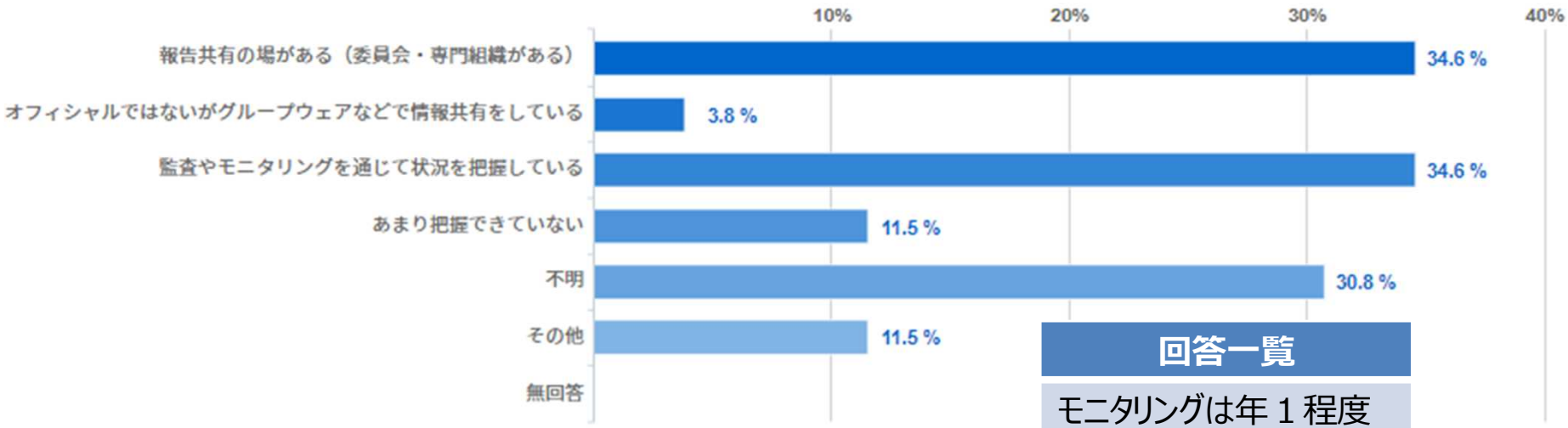
Q.6 情報セキュリティのガバナンスについて
ポリシー、規程類はどのように準備されていますか。



回答一覧
上位規定に基づき、各社独自の規定が作られる
会社ごとに異なる
子会社に関しては基盤となる奇蹄類は本社にて整備予定。その配下の細則や手順、ガイドラインは各子会社にて整備してもらう予定。
会社毎にガバナンスを実施
子会社は別のガバナンスだと思われる。

→やはり、本社や統括部門で取りまとめをしているというパターンが圧倒的であった。
　また、「他社、自部門以外の事情は把握していないという」という回答がゼロであったことから、何かしらの形でガバナンスを行う必要性があることはいずれの企業でも認知されていることがうかがえた。サプライチェーンマネジメント、セキュリティ／ガバナンスの観点からも統括部門やHQ等が管理していく流れが強くなると思われる。

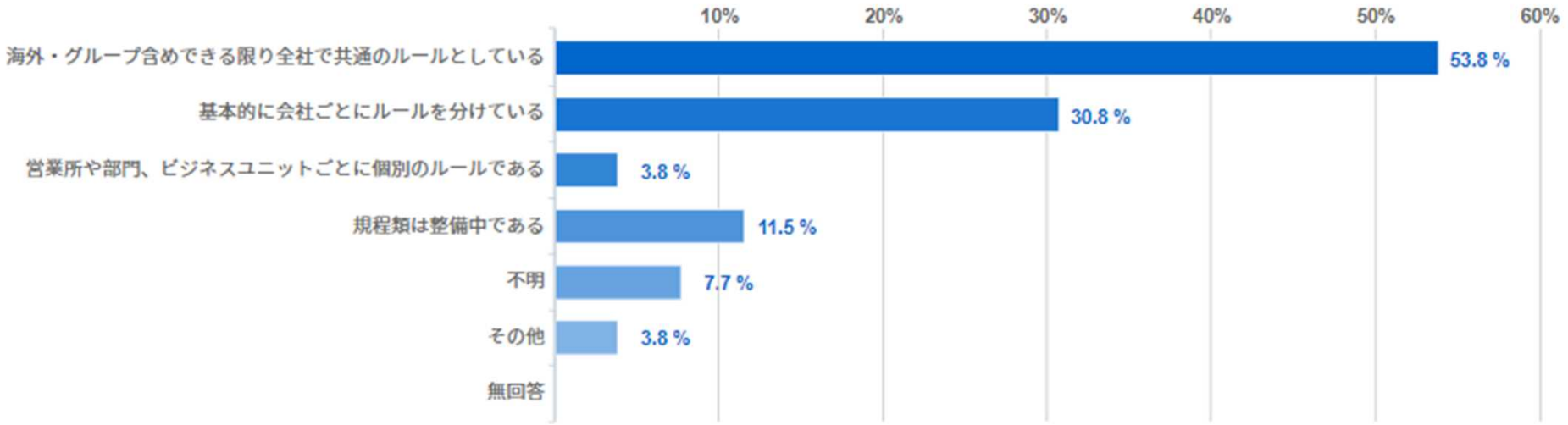
Q7. 海外拠点やグループ会社も管理している場合、各社の情報セキュリティの体制・状況をどのように確認していますか。



回答一覧
モニタリングは年１程度
定期的な調査

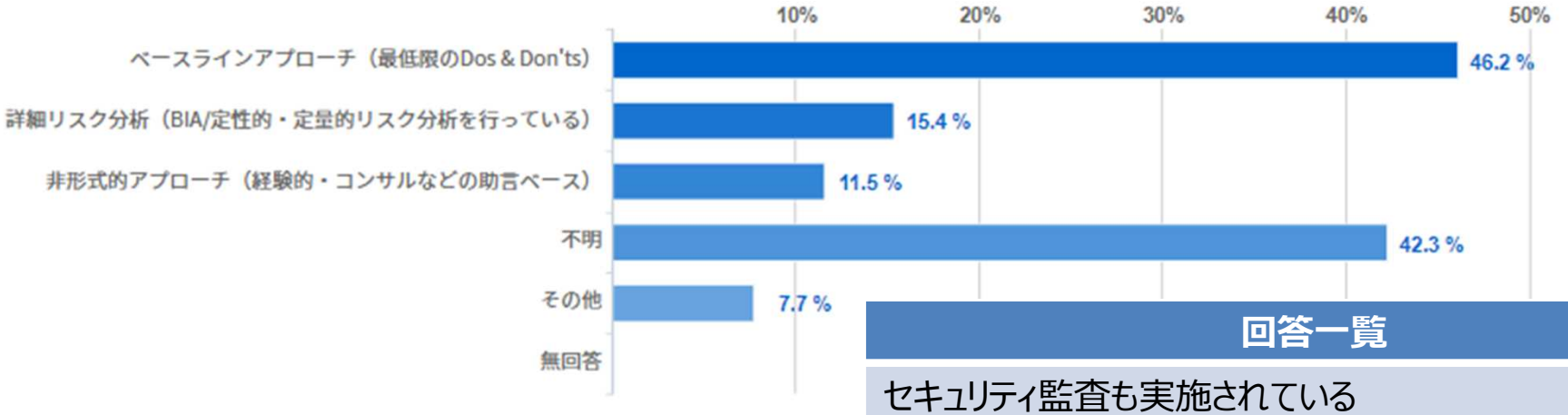
→情報共有の場や、モニタリングを通じて大多数の企業が他社の状況を把握しているといことがうかがえた。ガバナンスという性質上、アンオフィシャルな形での共有のプラットフォームはやや採用数が少ないようであった。

Q.8 情報セキュリティのガバナンスについて ポリシー、規程類の標準化などは行っておりますか。



→共通ルールとしているものが約半数であったが一方で、会社ごとにルールを分けているパターンも30%と、ポリシー・規程類の標準化・策定を行っている場合はこの2つのアプローチが大多数のようである。
一般的に、事業内容が全く異なる場合は違う規定にせざるを得ないパターンも多いために、そういったグループ会社を抱えている場合は後者のアプローチが多いのかもしれない。
事業内容、規模が異なる場合に共通ポリシーとすると、絵に描いた餅になりかねないために注意は必要である。

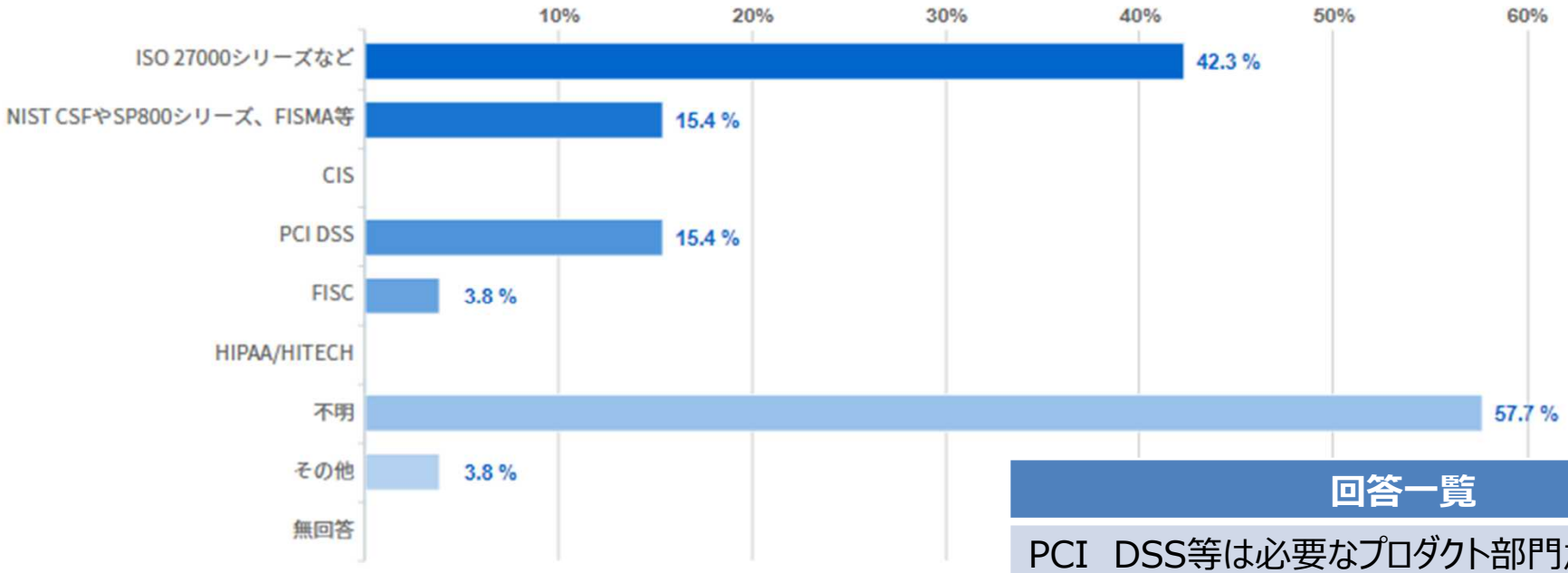
Q9. 海外拠点やグループ会社問わず、情報セキュリティのガバナンスについて主に、いずれのアプローチを採用していますか。



回答一覧
セキュリティ監査も実施されている
As Is、To Beそれぞれを定義し、その妥協点で定める予定

→ベースラインアプローチが最も多かった。詳細リスク分析まで行えている会社は、あまり多くないことがうかがえる。セキュリティ・リスクマネジメントの性質から言って、本来的には詳細リスク分析を行うことが望ましいとは言え、実行するには多大な労力が必要であるために、ベースラインからのアプローチが多いのかと推測される。
一方で「不明」の回答も多く、リスクマネジメントや規程類の制定を実際に行っている人間でないと回答がしにくい設問であったためと思われる。
またあまりに細かなポリシーを定めてしまうと、定期的な運用点検や監査対応といったPDCAが回りにくくなってしまう。そのため、定めたくても定められないのではないかといったことも考えられる。

Q10. 海外拠点やグループ会社問わず、情報セキュリティのガバナンスについて規格・フレームワーク・業界/法令に基づく標準等を採用されている場合、いずれを採用しておりますか。

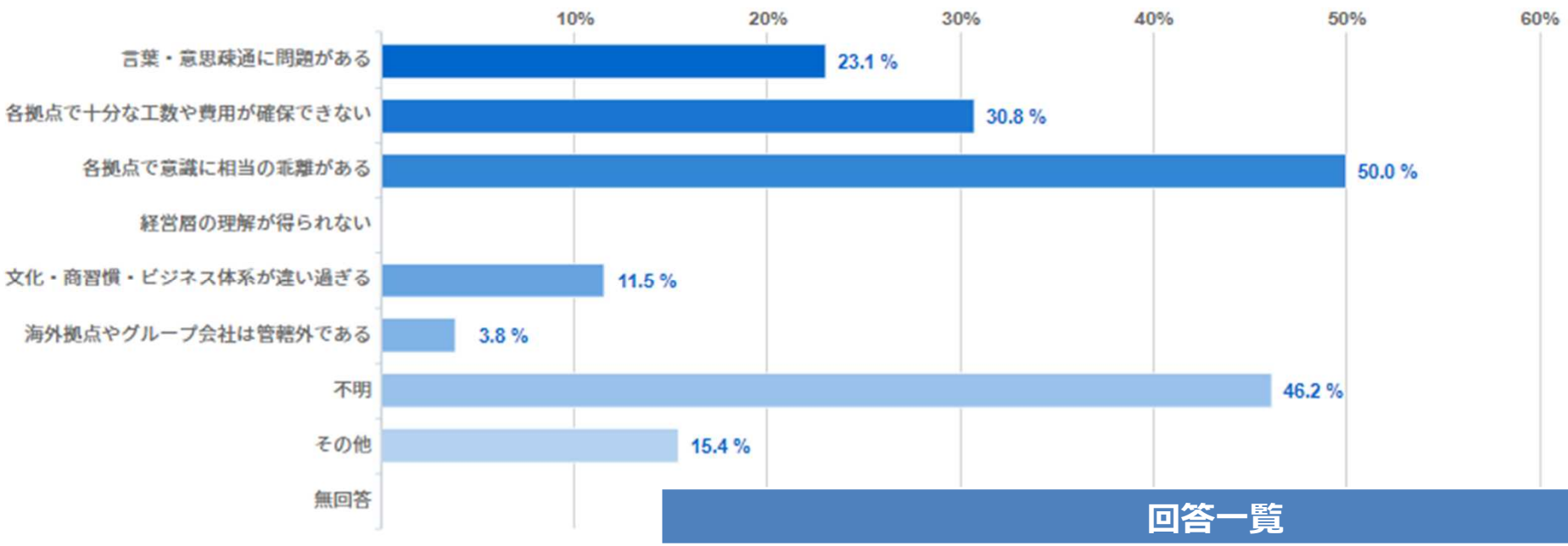


回答一覧

PCI　DSS等は必要なプロダクト部門が個別対応

→ISO27000シリーズが最も人気であった。日本企業ではISOの採用が多いと言われるが、如実に表れている。一方でNIST CSFや、PCI DSS、FISCなどの採用もあった。PCI DSSやFISCについては業界独特の要請によるものかと思われる。
また本設問でも「不明」の回答も多く、リスクマネジメントや規程類の制定を実際に行っている人間でないと回答がしにくい設問であったためと思われる。
冒頭に記載したように、NISTのSP800-171）については、防衛省と取引がある企業については、当該ガイドラインと同等以上のセキュリティレベルを満たす必要がある。そのため、今後はベンダの選定基準であったり、耳にする機会は増えると思われる。

Q11. 海外・グループ会社のガバナンスを進めようとされている、または進めたうえでの課題はなんですか



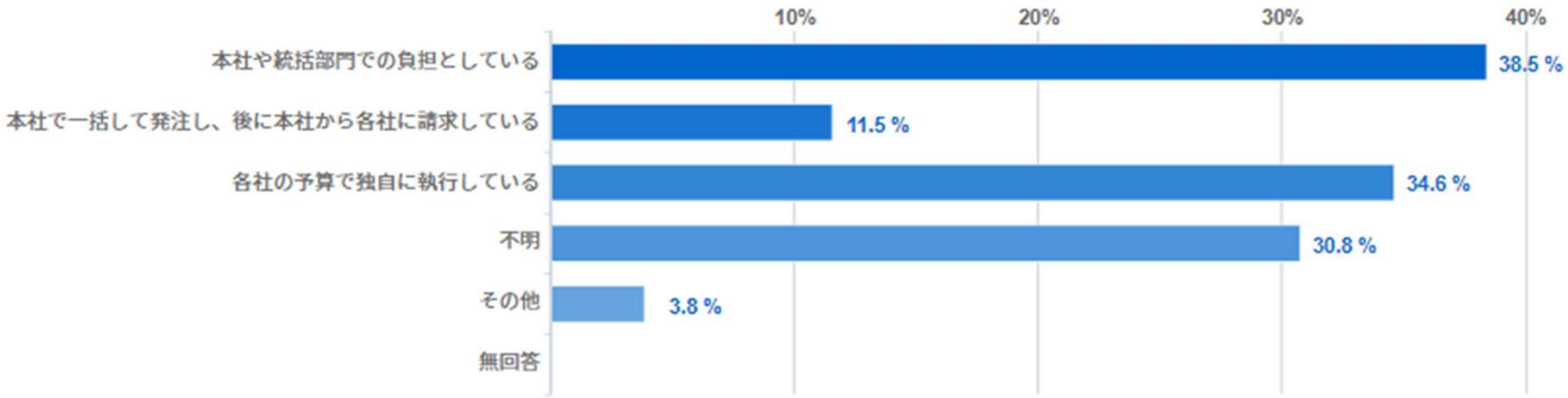
回答一覧

規模が国内／国外で違いすぎるため、絵に描いた餅にならないかが非常に心配

権限に関するルールが未整理で言うことを子会社が言うことを聞いてくれない。

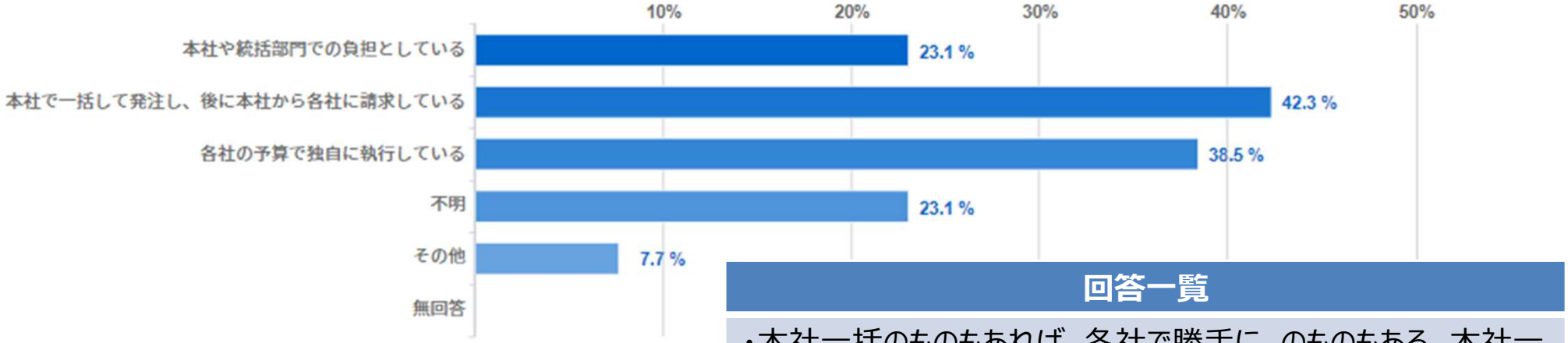
→各拠点での意識の乖離、という回答が50%を集めた。言葉・意思疎通の問題や費用の問題も決して少なくないが、思った以上にセキュリティの意識向上というものは海外拠点では問題になっているケースが多いようである。

Q12. 海外・グループ会社等のガバナンスの費用負担①
規程類の整備や体制整備について、費用負担はどのようにしていますか。（コンサル費、人件費等）



→Q13.と比較すると面白い結果となる。こちらの費用については、本社や統括部門での負担がトップで、次に各社の予算での執行となっている。本社での一括発注からの費用回収というパターンは少ない。Q13.では具体的な製品やライセンスなど按分しやすいために費用回収も可能だが、こちらではそれが難しいためにこのような形になっているものかと思われる。

Q13. 海外・グループ会社等のガバナンスの費用負担②
セキュリティソフトウェアやソリューションの導入費用・ライセンス費用について、費用負担はどのようにしていますか。

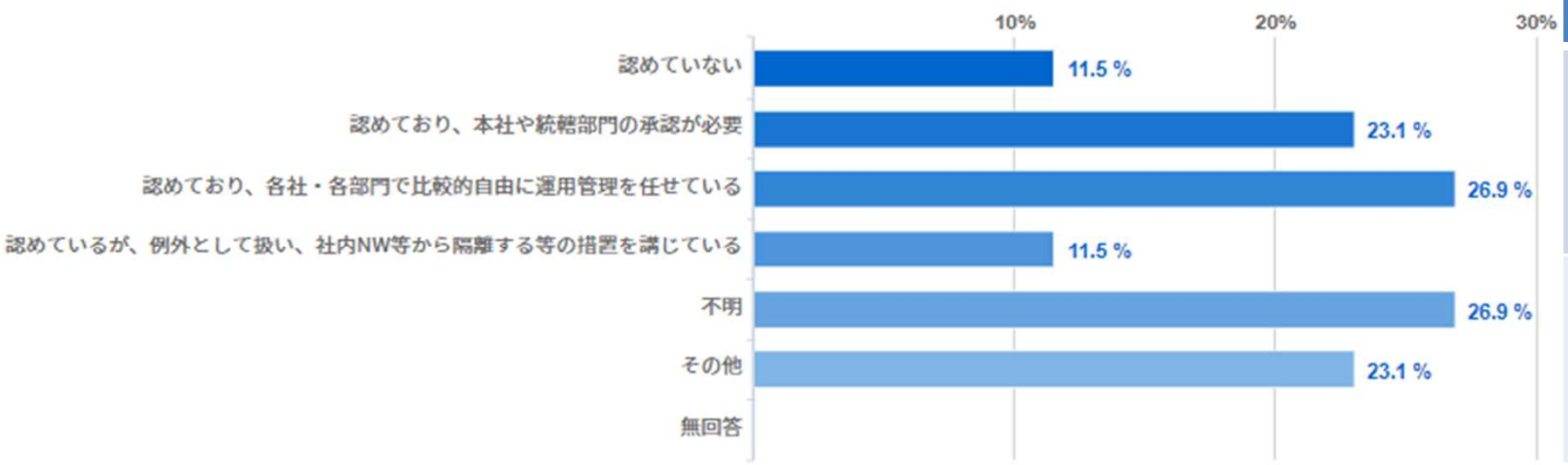


回答一覧

・本社一括のものもあれば、各社で勝手に、のものもある。本社一括→割り当てが統制的には良いが、管理工数が・・・　・弊社では、海外子会社のITインフラ費用は海外統括部門の費用負担となっているが、他社さんは費用負担はどうなのか？

→Q12.と比較すると面白い結果となる。こちらの費用については、本社での一括発注からの費用回収というパターンが最も多い。次点で、各社の予算での独自の執行となっている。こちらは具体的な製品やライセンスなど按分しやすいために費用回収も可能であるためかと思われる。加えて、ライセンス管理はコンプライアンスやガバナンスに直結しやすいこともあり、HQや統括部門で一元管理したい、といったコントロールも背景にあると思われる

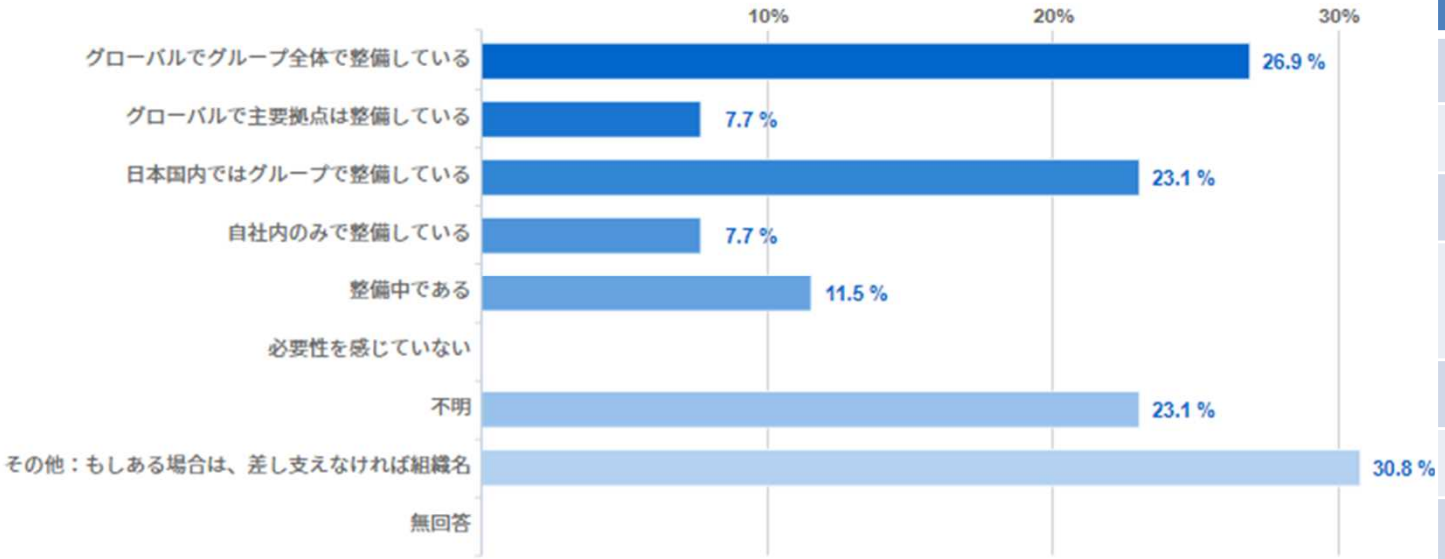
Q.14 海外・グループ会社の各社や各部門での独自のIT機器・サービス購入などを認めていますか。認めている場合、どのように制御していますか。



→本設問は非常に回答がばらついた。僅差ではあるものの独自の購入を認めており、自由に運用管理させているというものが最も多かった。一方で、本社や統括部門の承認が必要という回答も次点に来ており、ここは方針が大きく2つに分かれた。
認めている場合の管理策（計器棚卸等？）は非常に気になるところであったので、ここは設問に組み込んでもよかったかもしれない。

回答一覧
国内情報系は標準化。制御系並びに海外は管轄外（強制力が及ばない、状況も把握できない）
消耗品(マウスなど)の購入は自由に行わせ、独自のサービスを導入する際は統括部門に要相談というかたちにしている
システマチックに管理できていない。（棚卸を定期的に行ってはいるが、できている法人、できていない法人がある）
決められた範囲で自由に購買可能
認めていない(了承）ではなく、別の組織として関与していない。

Q15. CSIRTや類似の組織はありますか。また、もしある場合は、差し支えなければ組織名を「その他」欄で教えていただけますと幸いです。

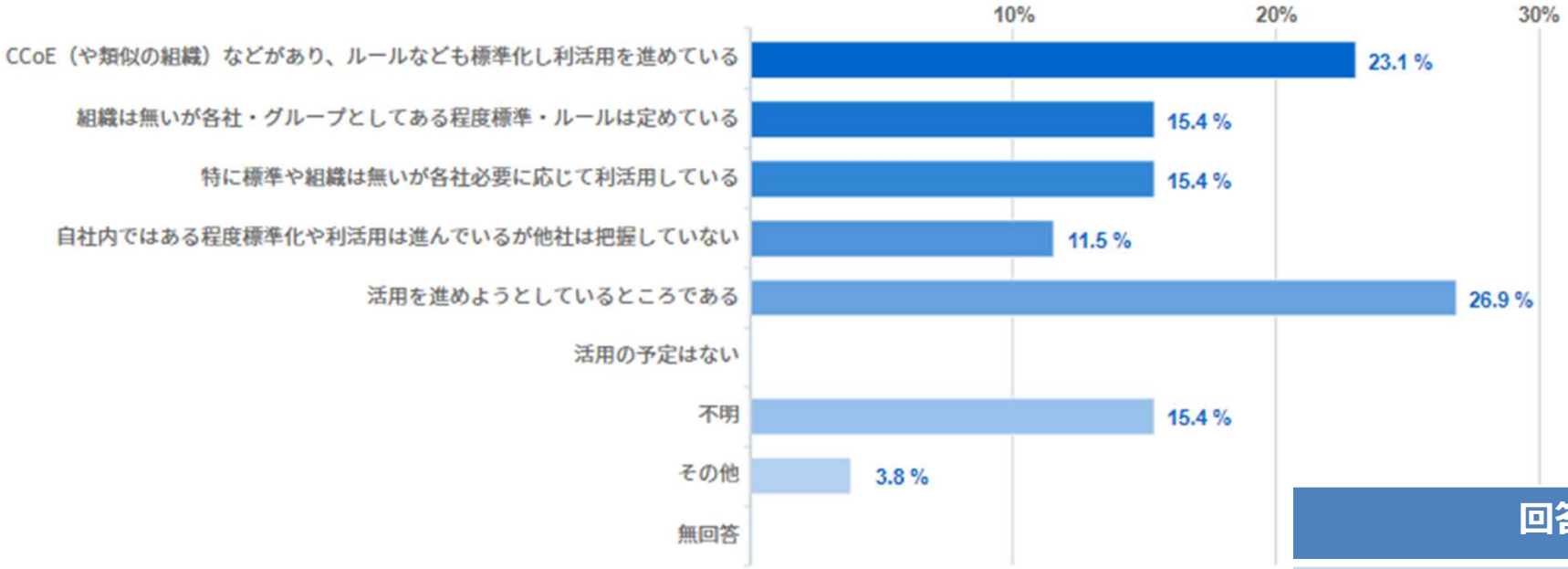


回答一覧
CSIRT,SOC
SOC
情報セキュリティ事故対応技術支援チーム
個人的にはない、と感じているが、上位層はある、と言っている「組織名：XXX-csirt」
なし
XXX CSIRT
XXX-SIRT
情報セキュリティ統括部

※企業名が入っている部分は「XXX」でマスキングしました。

→本設問も、あまり一か所に固まってはいないものの、グローバルかつグループ全体で整備している会社が25%を超える等、グローバルでのガバナンスがやや一般化しつつあるということがうかがえる。また、「必要性を感じていない」についてはゼロであり、何かしらの形でこういった組織の整備にいずれの企業も取り組んでいることがうかがえた。

Q16. 海外拠点やグループ会社問わず、(主にパブリック)クラウドの利活用とその統制についてどのように行っていますか

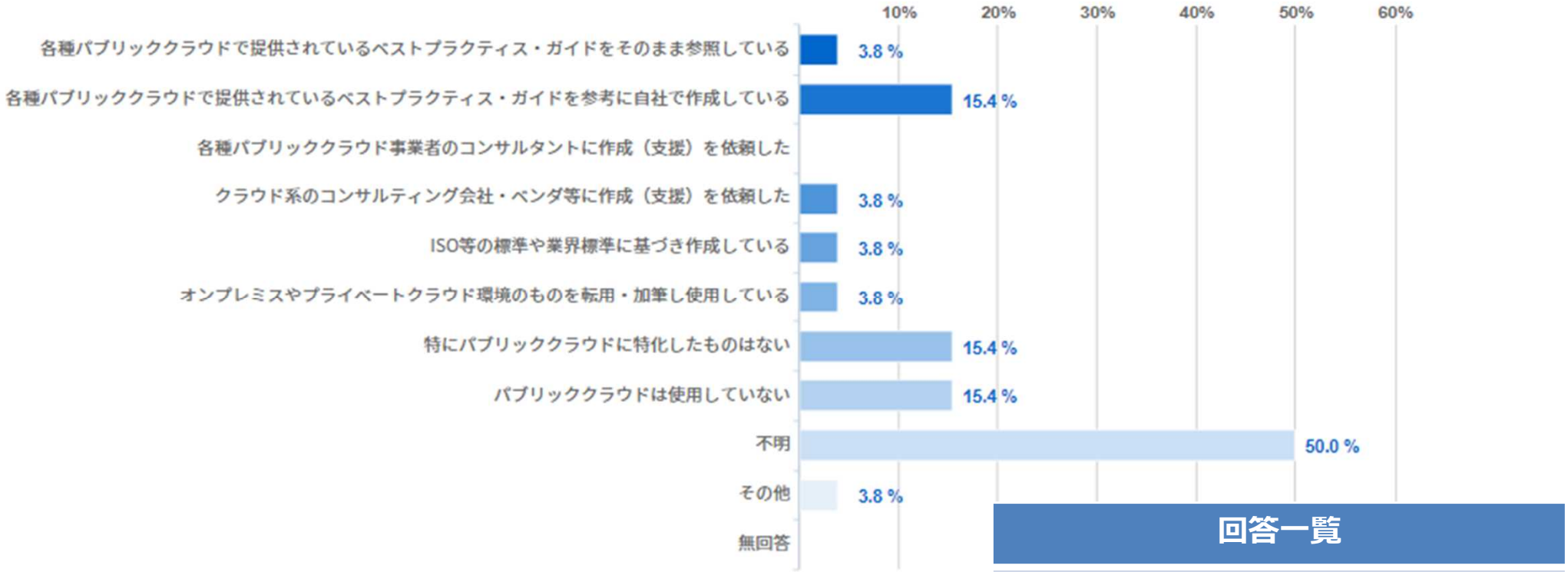


回答一覧

活用推進と把握方法の体制を構築中

→本設問も、やや回答がばらついているものの、既にCCoEのような組織を作っている企業も少なくなく、また、「活用の予定はない」がゼロであることからルール策定状況はまばらではあるものの、パブリッククラウドの利活用は進んでいることがうかがえる。
CCoEについては興味を示している企業が多いかと思われるので、実際に設立している企業については具体的な取り組み策などをヒアリングできるように設問を組み込んでもよかったかもしれない。

Q17. 海外拠点やグループ会社問わず、パブリッククラウドをお使いの場合で、パブリッククラウドのセキュリティ対策の標準（規程・ルール）がある場合、どのように作成されました。（これから作成する場合、どのように作成される予定ですか。）

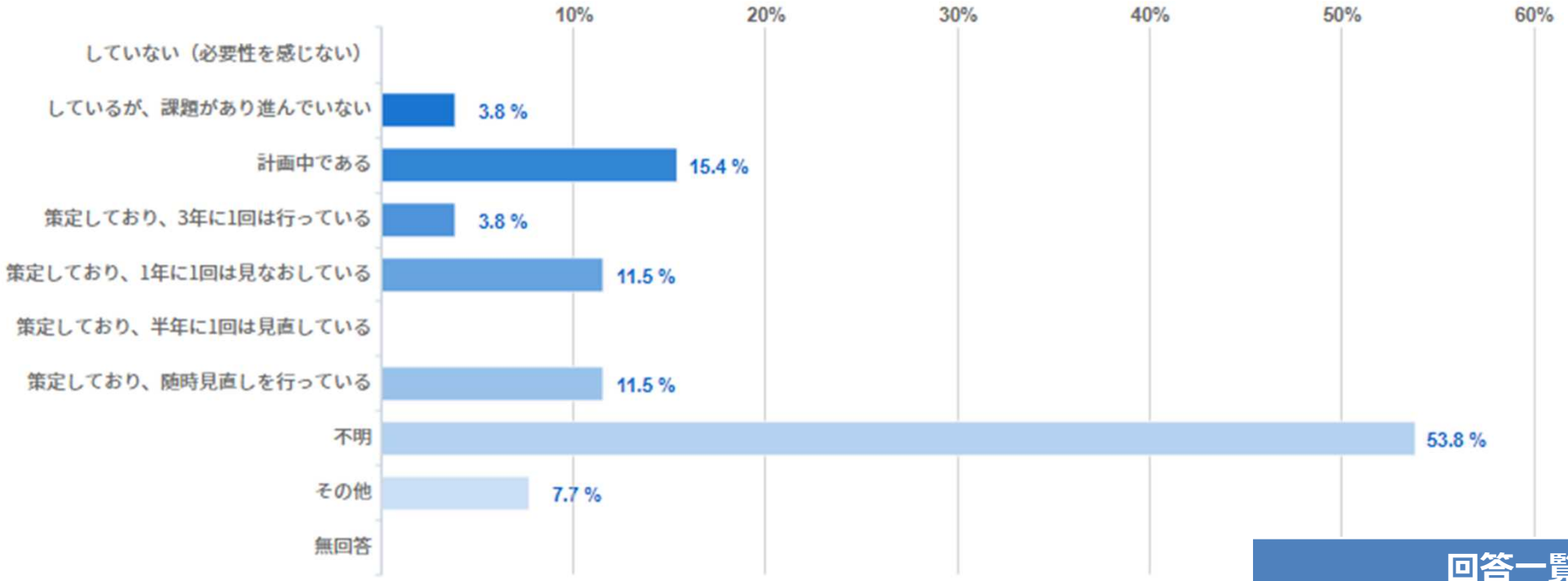


回答一覧

持株ホールディングスでガイドを作成し展開

→本設問も、やや回答がばらついている。現状、作成している企業の中では各種パブリッククラウドで提供されるベストプラクティス・ガイドを参考に自社向けにテーラリングしているパターンが一般的なようである。

Q18. 海外・グループ会社等含め、グローバルポリシーを策定していますか？（セキュリティ、インフラ整備等）整備している場合、見直し頻度はどのくらいですか。



回答一覧
組織再編に伴い整備中

→本設問も、やや回答がばらついている。見直しをしている場合は、1年に1回や都度見直しが比較的多かった。本設問も、「不明」が多く、具体的にポリシー策定や改定に関わっている人間でないと回答しにくいことがうかがえた。

Q.19 運用開始までで苦労した点はありますか？

回答一覧
CSIRT室、全社を統合するシステム部が統率しているので、特にありません
現在関わっているパブリッククラウド向けの規程策定では、既に存在していたオンプレ向けの規程内容が全く流用できず、策定にかかわる人の意識を変える(境界防御の考え方では通用しない)事から始めていく必要があった。
海外やグループ会社はネットワーク構成が把握できないケースが多く、インフラの可視化から入る。そこで問題点を指摘し標準化に持ってゆく。
海外Gr方針/実施及び前段の説明
言うことを聞かない組織・部署・会社の取り扱い

→「ありがち」な事項が挙げられた。海外やグループ会社においてはそもそも構成が不明瞭であったり、または方針についての説得や意識合わせが課題となるようなケースが、他社でも見られたようであった。冒頭でも記したように、やはり管理部門としての手間を減らすのであればできる限りコストが許す範囲でシステム環境などは統一したほうが管理はしやすいだろう。

Q20. ・規程類は、AS-ISで作成しましたか、TO-BEで作成しましたか。
・また作成（骨子作成、ドキュメントの体裁整備）にかかった期間はどのくらいですか？
・作成後、周知展開にかかった期間を教えてください。

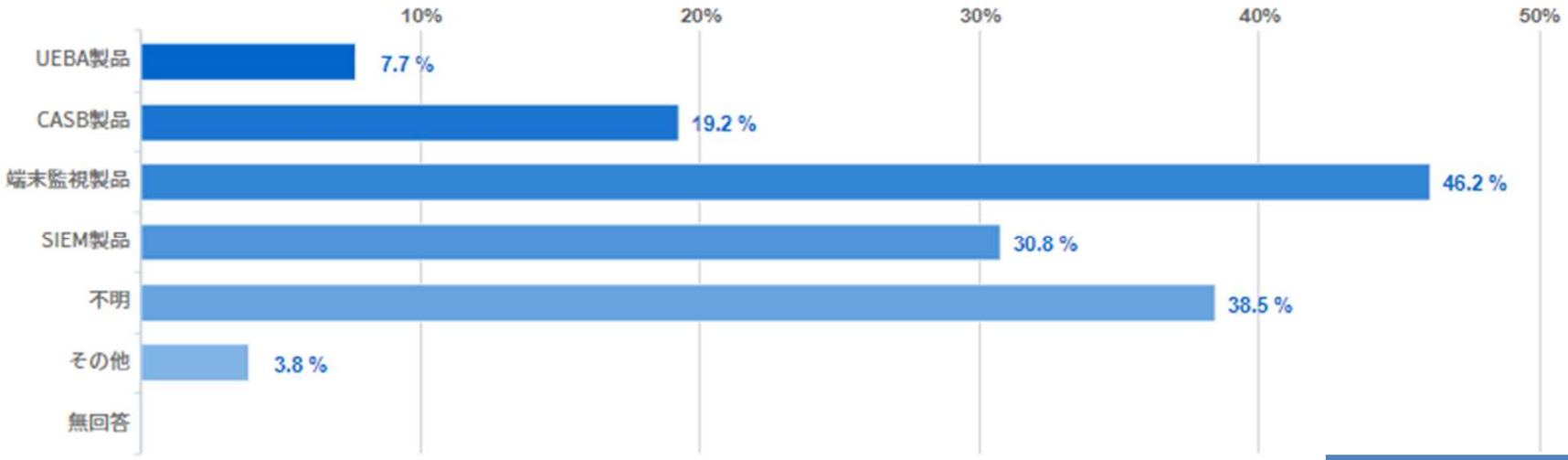
回答一覧
わかりません
(現在策定しているパブリッククラウド向けの規程) 規程内容はTo-Be、ドキュメントの体裁はAs-Isで作成している。
現在守るべきルールとしてAS-ISだと言える。将来の変動については改訂で対応する。
TO-BEを作ってからAI-ISとのフィッティングを評価して内容微調整
不明

回答一覧
わかりません
(現在策定しているパブリッククラウド向けの規程)　5か月程度
不明
不明
一年程度

回答一覧
わかりません
周知展開は2週間程度だが、新しい規程内容にシステムの是正する猶予期間として1年程度が設けられる。
ヘッドクォータから公文書として発信したら施行。
半年程度
不明

→有効回答数が多くなかったものの、どちらかというとTO-BEで作成している企業が多い。または、AS-ISで作成したとしても改定を計画していることからやはり継続的見直しをしていく形かとは思われる。
規程作成には半年～1年という回答であった。新規作成かつコンサルなどを入れる場合はそれなりに長期間（最低でも3か月程度）は見ておくのが安全かとは思われるが、想定以上に長い期間を要することが分かった。
また、周知に関してはそれ自体は短くともリリースする内容次第で既存システムに影響が大きい場合十分な猶予期間を設けておくというのは計画に入れておくべきだろう。

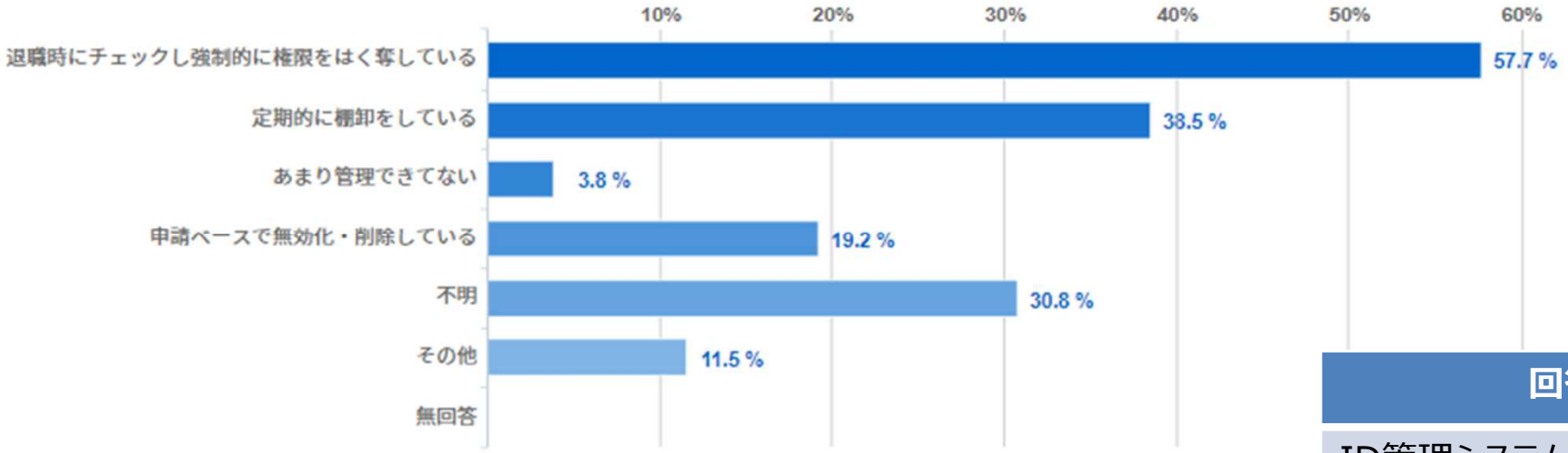
Q21. 海外拠点やグループ会社問わず、内部不正対策は何か行っておりますか。IT技術を投入している場合はどのようなものを入れているのかご教示ください



回答一覧
UEBA,CASB,SIEMを検討中

→「不明」という回答も多かったが、内部不正対策自体は何らかの形で行っている企業が多いことがうかがえた。端末監視系のソフトがまだトップではあるものの、3割近くの企業でSIEMを導入しており、新技術も徐々に浸透してきているようである。一方で、UEBAまで導入している企業はまだ少数であることが分かった。

Q22. 海外拠点やグループ会社問わず、退職者管理はどのように行っていますか。



回答一覧
ID管理システムでひも付く権限は一括抹消される。証明書など含め。
海外拠点は管理できていない。
一部システムは独自管理

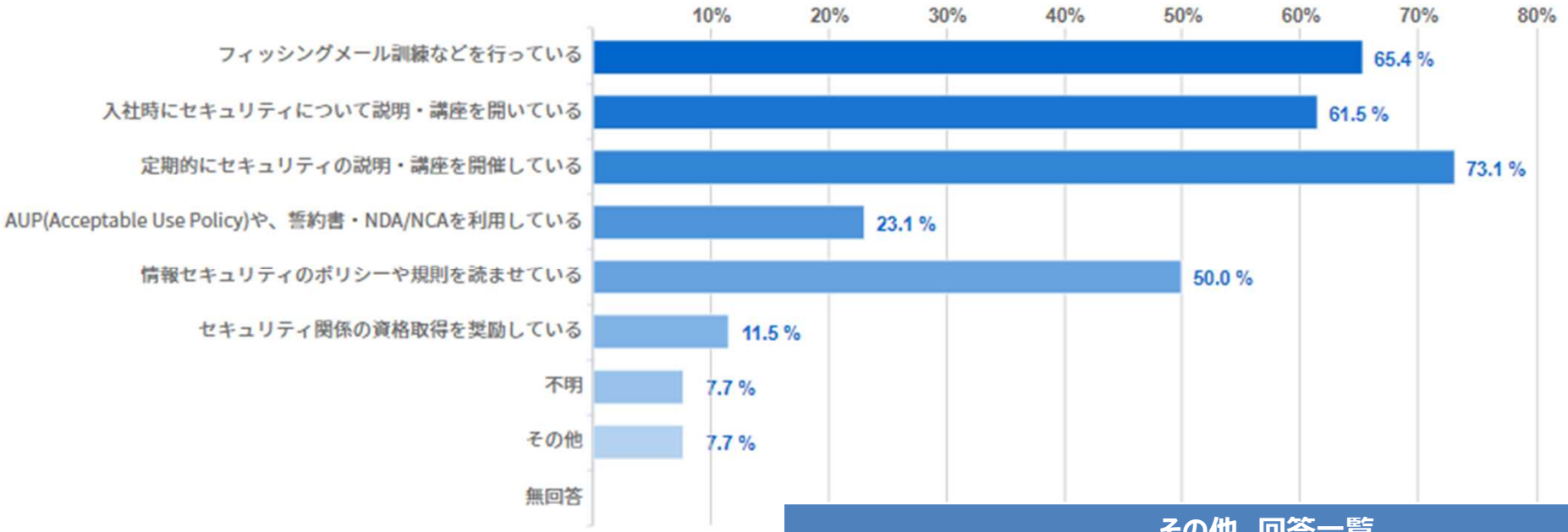
→退職時に強制的に権限はく奪をしている企業が過半数であった。また、定期的な棚卸を行っている企業も40%近くになっていた。「あまり管理できていない」企業は3.8%と、各企業退職者管理は行っていることがうかがえた。

Q23. 全社的統制を図るための点検、権限管理等はどのように行っていますか。

回答一覧	
CSIRT, アシュアランス室が監査を定期的にしています。	月次でセキュリティ担当社員が確認を行っている。
特権IDはWorkflowシステム払い出しとしている。 2要素認証の適用を考えている。	権限マトリクスによる管理、閲覧権限システムによる権限管理、定期的な棚卸
年に1度、IT統制の点検があり、システム毎に確認、証跡を提示している。	ガバナンスの担当部署が定期的にリスクアセスメントを実施
本社部門にセキュリティ担当チーム（子会社委託）があり、各種振舞や外部のセキュリティインシデントIPA情報などを監視・報告している。	社内セキュリティルールによる規程を定めて管理 セキュリティ部門がアセスメントを実行　*新規開発時
不明	提起棚卸
グループリスク管理部門から年次内部監査	原則管理者権限は与えていない。申請による一時の申請のみ。
組織規程、職務権限規定等で定められている、人事システムで権限管理している。	定期的な監査等で点検を実施。
権限（サーバーへのアクセス権）管理は、Excelに権限情報をまとめ、年2回棚卸対応を行っている	

→予想はしていたが、年数回の定期棚卸・監査をしている会社が多数であることが分かった。一方で二要素認証の導入を検討している企業もあった。特に特権については内部不正・外部からの攻撃での悪用でリスクが高いアカウントであるために、今後ゼロトラストへのシフトが進む場合は適切かつよりタイムリーなアクセスコントールが求められるだろう。

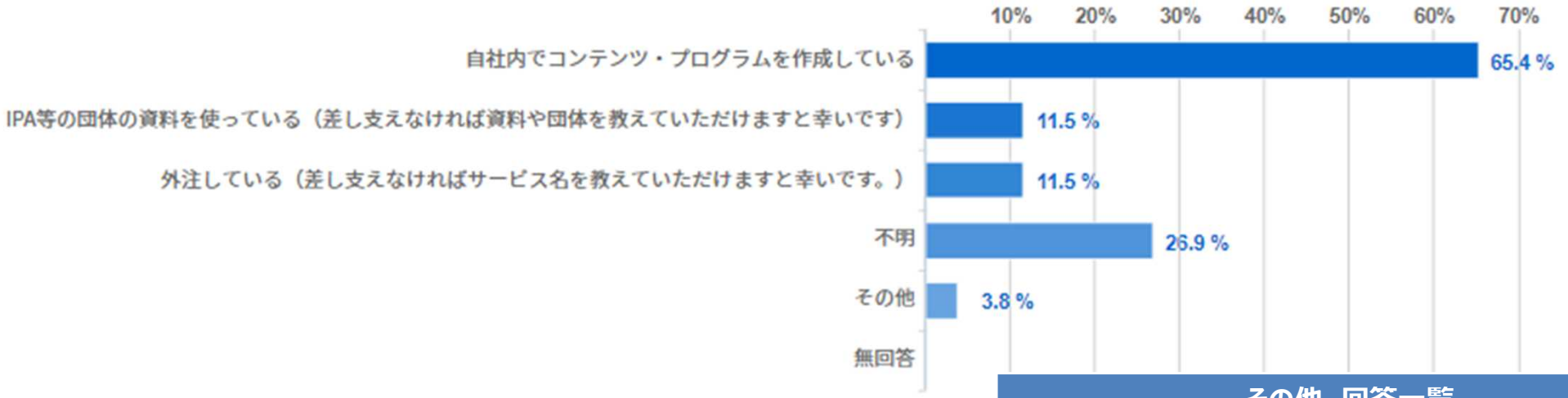
Q24. 海外拠点やグループ会社問わず、(一般)従業員のセキュリティの教育はどのように行っておりますか。



その他　回答一覧	
国内に限り、定期的な点検を実施している	e-ラーニングで定期的にチェック

→フィッシングメール訓練や、入社時・定期的なセキュリティ講座等の対応は多くの企業で行っていることがわかった。

Q25. 海外拠点やグループ会社問わず、(一般)従業員のセキュリティの教育のコンテンツはどのように準備されておりますか。

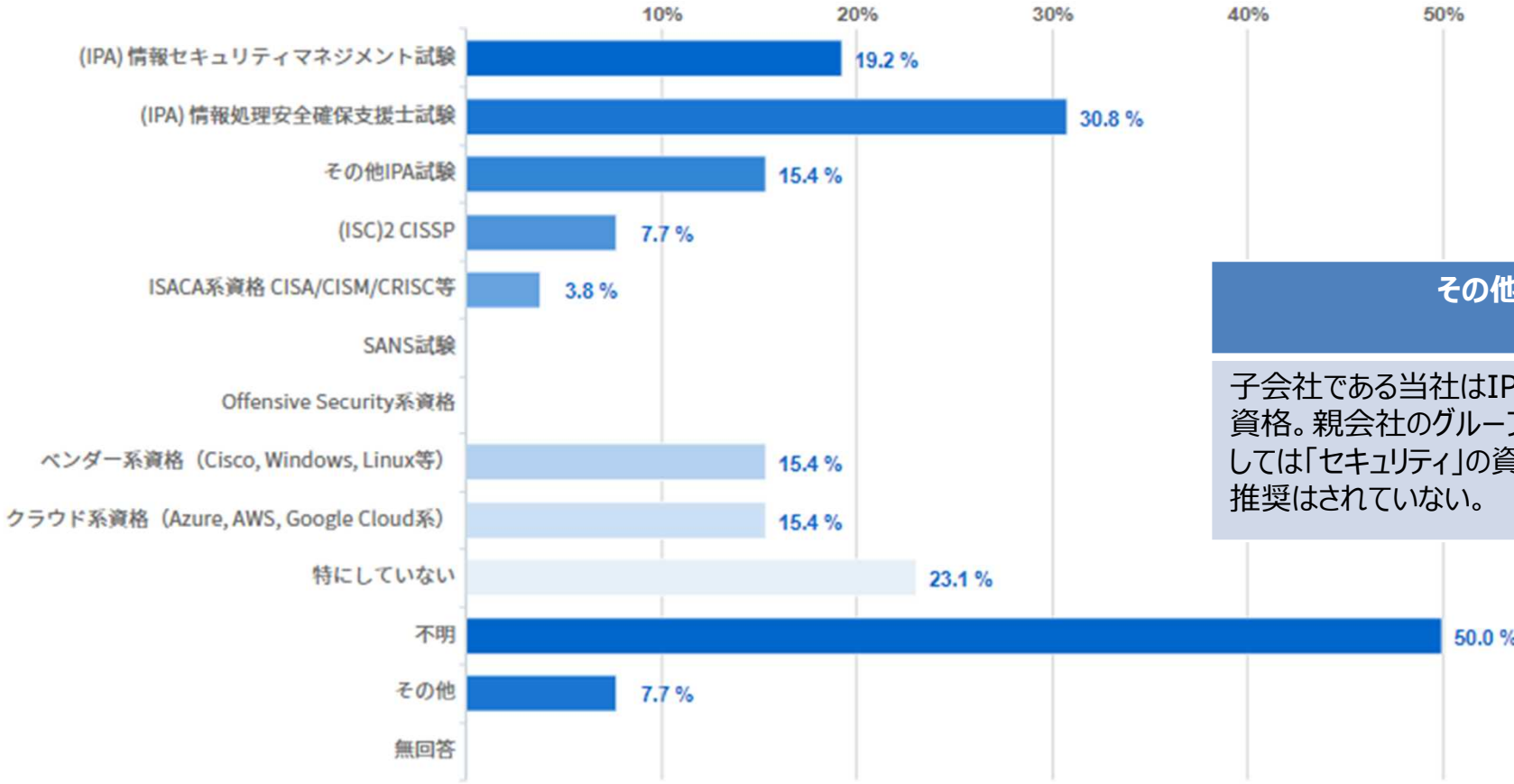


その他　回答一覧

メール訓練：ラックのメール訓練サービスを利用。脆弱性診断サービスは以前,TISを利用していたが、別のものを検討中

→内製しているという回答が圧倒的であった。外部資料を用いたり、外注まで行っているパターンは、あまり多くないようである。

Q26. 海外拠点やグループ会社問わず、情報セキュリティのガバナンス業務実務者や関係者の育成について資格取得を奨励していますか。その場合、どのような資格を奨励していますか。

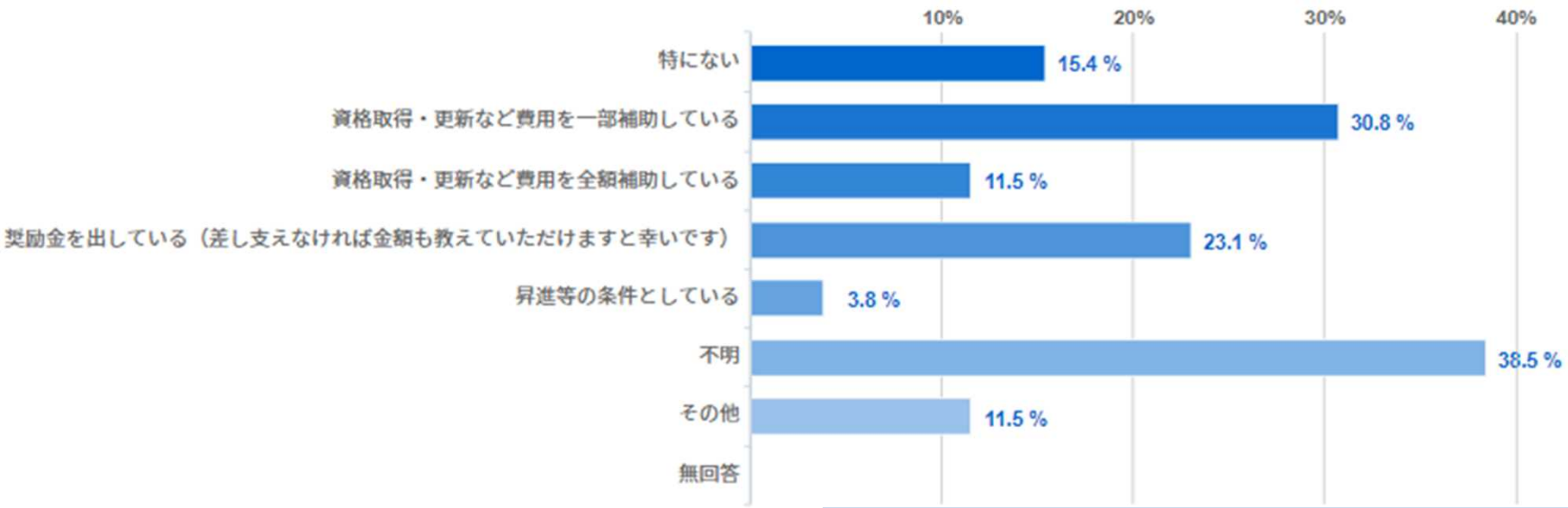


その他　回答一覧

子会社である当社はIPA資格。親会社のグループとしては「セキュリティ」の資格推奨はされていない。	各種資格をグレード設定し、グループ会社内で独自の資格体系ランクを設定している

→「不明」が多いものの、全体としてはIPA系の資格の採用が多いようであった。特に情報処理安全確保支援士は約3割の企業で採用しているようである。グローバルのセキュリティ資格（ISC2やISACA, SANS等の資格）は採用が少ないようである。

Q27. 海外拠点やグループ会社問わず、情報セキュリティのガバナンス業務実務者や関係者の育成について資格取得を奨励している場合、どのようなインセンティブがありますか。



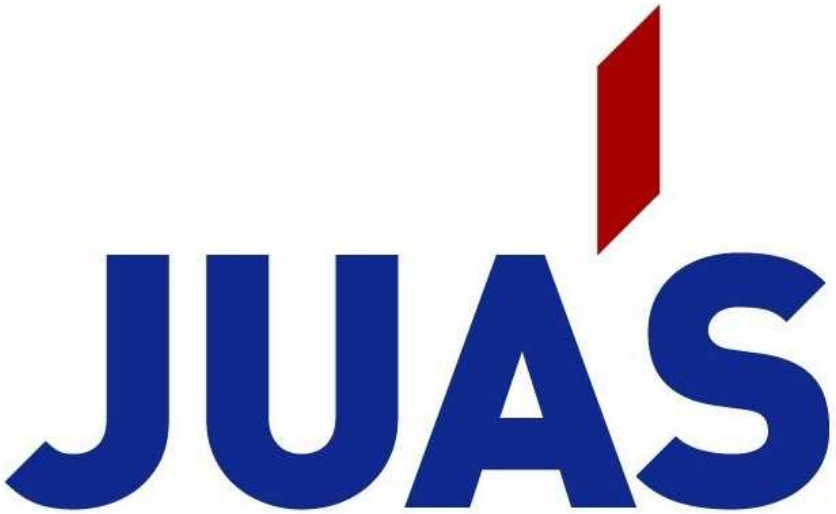
その他　回答一覧	
（セキュリティだからというよりも、IPAの資格が無いと各段階での昇格ができない）	グループ会社内独自資格体系でのランク付けを用意
高度資格は一時金20万	

→同様に「不明」が多いものの、全体としては補助や報奨金を出すといった対応をしている企業の方が割合は多いようである。報奨金として、（恐らくはIPAの）高度資格では一時金として20万円を支給しているといった企業も見受けられた。

謝辞：重ねて、ありがとうございました。

以上、27問となります。

改めまして、今年の参加の皆様、アンケート調査へのご協力、本当にありがとうございました。お礼申し上げます。


JUAS