2023年度 ITインフラ研究会
活動成果報告

2024年4月11日(水)

ITインフラ研究会

2023年度 ITインフラ研究会　～分科会テーマ～

分科会1	新規システム構築・システム更改時におけるオンプレ・クラウド選定基準
分科会2	ゼロトラストを知ってますか？
分科会3	理想の共通インフラ基盤の構成とは ―クラウド化が進む中で現状の構成はどうあるべきか
分科会4	インフラ開発案件リリースに向けた品質向上施策における研究 ―レビューで安心・安全なITインフラを創る
分科会5	業務標準化を目的としたAIによる自動ドキュメント化
分科会6	ITインフラの事業継続計画について

2023年度 ITインフラ研究会
分科会1

新規システム構築・システム更改時における オンプレ・クラウド選定基準

資料目次

- テーマ選定に至った背景・経緯
- アンケート概要/結果/考察
- システム構築時におけるオンプレ・クラウド選定の判断基準
- まとめ

2024年4月

分科会1

テーマ選定に至った背景・経緯

■各自のお悩み相談会のテーマから研究会テーマを選定

マルチベンダ化に対する統制管理について

テスト環境運用について

A）社内コミュニケーションツール使い分け
（B）社内ITツール・サービス活用促進の方法

次期PBXのあるべき姿

グループ標準パブリッククラウドにおけるガバナンス・活用促進

どこまで先の、誰にとっての、あるべき姿を検討してシステム企画を実施しているか？

自社で備えておくべきITインフラについて

テーマがみんなバラバラ‥
興味はみんなあるけど研究テーマとしては
自社の状況にはそぐわないものが多い‥

クラウドというキーワードだと
各自何かしら課題感や興味があるかも

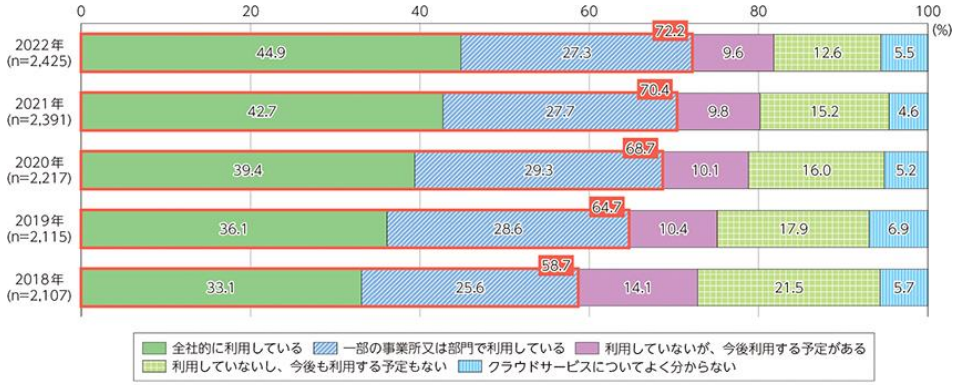
クラウド　をキーワードに研究テーマを深堀

テーマ選定に至った背景・経緯

■クラウドが普及して時間が経つが、今どのくらい普及している？

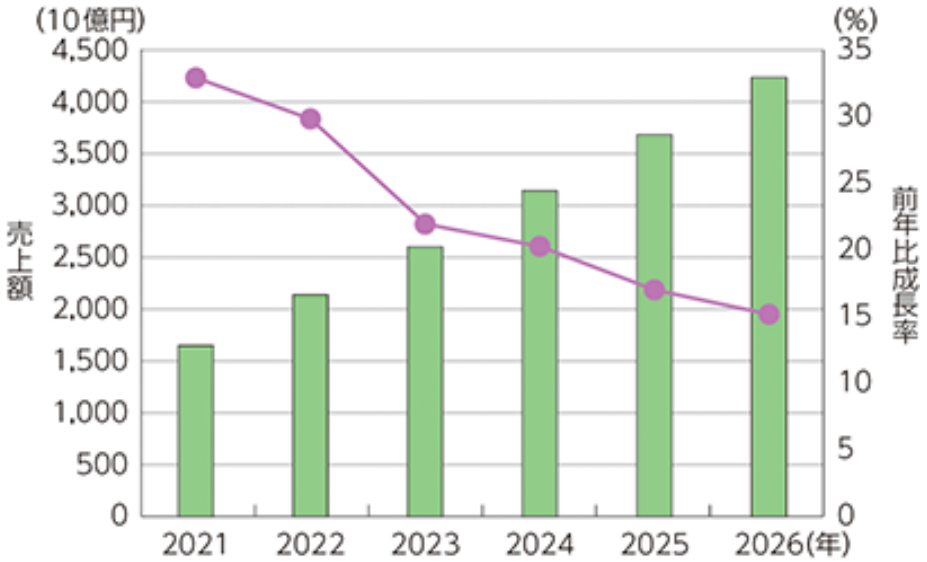
✓ 2022年時点で **約7割** の企業が クラウドサービスを利用しており、年々増加している

国内のパブリッククラウド市場も拡大しており、国内の多くの企業がクラウド移行していることが窺える



	集計企業数	比重調整後集計企業数	クラウドサービスの利用状況							
			利用している	全社的に利用している	一部の事業所又は部門で利用している	利用していない	利用していないが、今後利用する予定がある	利用していないし、今後も利用する予定もない	クラウドサービスについてよく分からない	無回答
全 体	2,428	2,428	1,749	1,087	662	539	233	306	134	6
[産業分類]										
建設業	368	102	86	55	31	14	8	6	2	－
製造業	387	639	455	271	183	153	85	68	28	4
運輸業・郵便業	408	227	145	77	67	70	30	40	12	－
卸売・小売業	364	489	377	245	133	91	35	55	21	－
金融・保険業	165	29	27	21	6	2	1	1	0	－
不動産業	159	38	32	25	7	4	1	3	2	－
情報通信業	257	132	123	101	22	9	5	4	1	－
サービス業、その他	320	772	505	293	213	197	68	129	68	2

クラウドサービス利用状況



日本のパブリッククラウドサービス市場規模(売上高)の推移及び予測

出典：総務省｜令和5年版 情報通信白書｜データ集（soumu.go.jp）

テーマ選定に至った背景・経緯

■一般的にオンプレミス・クラウドのメリット・デメリットは以下の通り。

項目	オンプレミス	クラウド
コスト	ハードウェアの購入・保守、設備の維持管理が必要	初期投資が低く、利用量に応じて課金可能
柔軟性	拡張や変更には物理的な資産の追加や交換が必要	リソースのスケーリングが柔軟で容易
運用管理	自社で管理・運用が必要、スタッフのトレーニングが必要	プロバイダによる運用、自動化が進んでいる
セキュリティ	ファイアウォールやセキュリティ対策を独自に構築・維持	クラウドプロバイダによるセキュリティ機能を利用
パフォーマンス	ハードウェアの性能に依存	プロバイダが提供する高性能なリソースを利用可能
アップデート	システムのアップデートは自社で行う必要あり	プロバイダがシステムのアップデートを担当
可用性	自社で冗長性を構築する必要あり	プロバイダが冗長性や可用性を提供
ネットワーク	自社でネットワーク構築・維持が必要	プロバイダのグローバルネットワークを利用

※上表はChatGPTからの回答

テーマ選定に至った背景・経緯

■各社の基盤構成についてディスカッション

各社それぞれの事情を抱え、試行錯誤をしながら最適な基盤構成を模索している
クラウドへ移行・運用して1サイクル経った企業が多い今だからこそ
「研究会参加各社のメンバーに対してアンケート」 ＋ 「分科会メンバー内でディスカッション」 を行い
オンプレ・クラウドそれぞれの特性を再確認し、選定の助けとなる基準を提起する

新規システム構築・システム更改時におけるオンプレ・クラウド選定基準

アンケート

ITインフラ研究会の参加者を対象に、社内のオンプレ・クラウドの選定に関するアンケートを行った。(回答者：24名)
アンケートでの主な内容は次のとおり。

- ○ システム導入時における社内のオンプレ・クラウド選定の方針について
- ○ 各システム分類におけるシステムの導入方式(オンプレ又はクラウド)について
- ○ システム導入時における社内のオンプレ・クラウド選定基準の有無とその内容　等

表　システム分類の例

選択肢	銀行での例
(1) 財務会計システム	決算システム、経費精算システムなど
(2) 人事給与システム	人事評価、勤怠管理システムなど
(3) 基幹系・業務系システム（企業の経営に直結するシステム）	勘定系システム、ATM中継システムなど
(4) 情報系システム	メール、社内ポータル、スケジュール共有など
(5) データ保管系システム	ファイル保管、データ共有など
(6) 顧客向けシステム	ATM、インターネットバンキング(個人、法人)、銀行アプリなど
(7) 共通基盤システム	認証(ドメコン)、ID管理など
(8) セキュリティシステム	アンチウィルス、パッチ管理、ログ管理など

表　自由記述の理由の分類

分類（※）	内容
(1) 可用性	システムの安定稼働、災害時での継続利用などを理由とした記述
(2) 性能・拡張性	性能面、リソース拡張、パフォーマンスなどを理由とした記述
(3) 運用・保守性	運用・保守の効率性、時間帯、障害児の対応などを理由とした記述
(4) セキュリティ	データの気密性、情報漏洩リスクなどを理由とした記述
(5) 移行性	システムの構築期間、各システムの互換性などを理由とした記述
(6) コスト	コストを理由とした記述
(7) システム環境	システムを設置する環境、エコロジーなどを理由とした記述
(8) 社内資産	人材育成、リソースの向上などを理由とした記述
(9) その他	アンチウィルス、パッチ管理、ログ管理など

※　非機能要求グレード2018を参考に設定

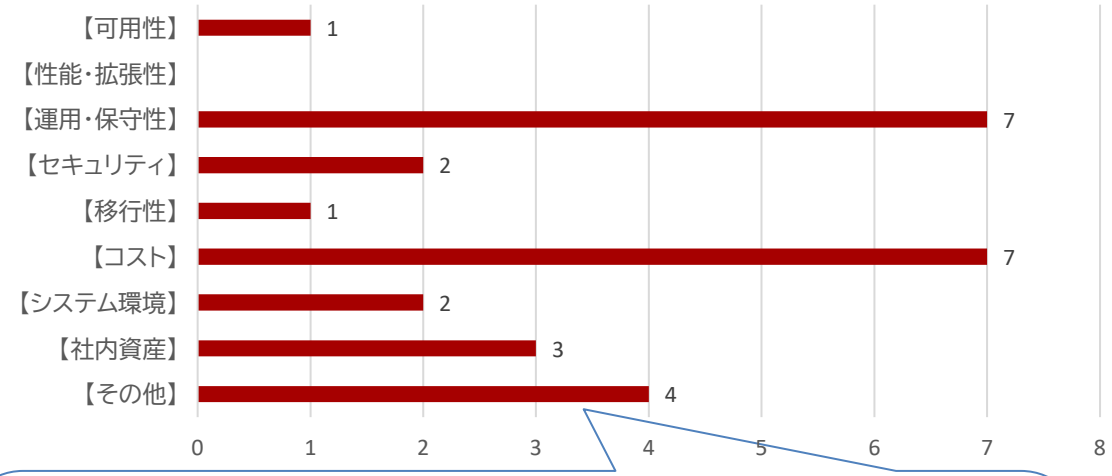
クラウドファーストとは？

企業や官庁などの組織が情報システムを導入あるいは更新する際、その運用基盤としてクラウドサービスの利用を第一に検討するべきとする考え方。独自にアプリケーションを開発せず事業者が提供しているSaaSを導入・利用したり、開発したシステムを事業者が提供するIaaS/PaaS上で運用するシステム形態を優先的に検討することを指す。

アンケート①:クラウドファースト方針の対比

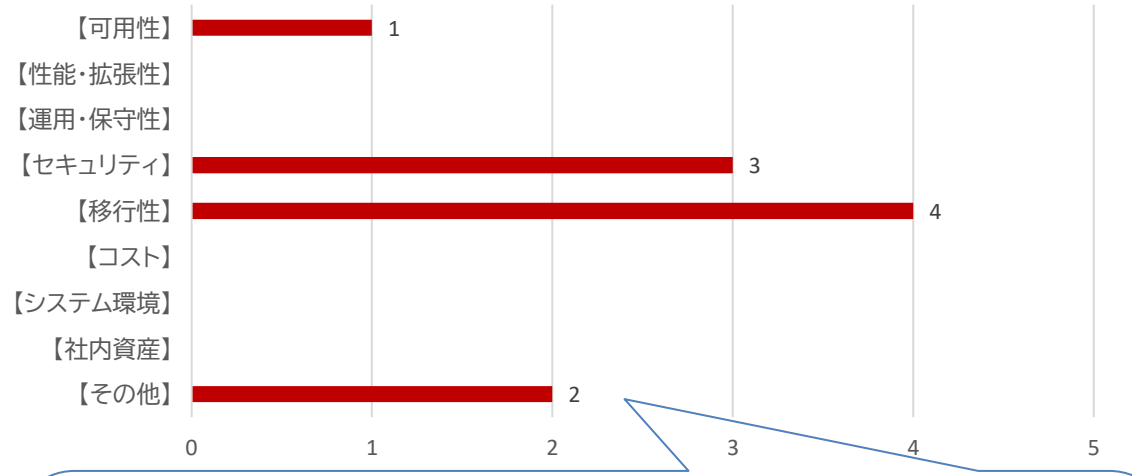
「クラウドファースト方針」とそうでない場合、どのような理由が背景にあるのか、対比から見えるものは

クラウドファーストの理由　N=17



- 運用管理手間・費用を抑制したい。【運用・保守性】【コスト】
- 既存データセンター内の構成が増改築を繰り返した結果、誰もわからない事になっているため【運用・保守性】
- ITトータルコスト削減やアウトソーシング等によるITマネジメントの標準化、業務効率化及び人材の高度化などに寄与する施策として重要な位置づけとして取り組んでいるため。【コスト】【運用・保守性】【社内資産】　等

クラウドファーストとまでは言えない理由　N=7



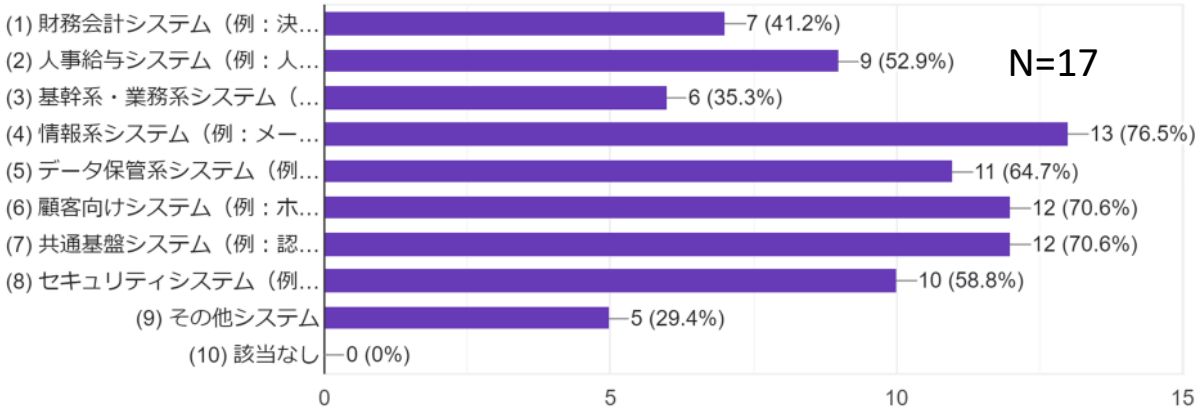
- 機微な情報が多く、方針転換するための環境が整っていないため【セキュリティ】【移行性】
- 社内オンプレによる仮想基盤がきちんと整備されており、必ずしもクラウド移行のメリットが得られるシステムがあるわけではないため【移行性】
- クラウド化できない古いホスト系のシステムがあるため【移行性】　等

- クラウドファースト方針であるとの回答からは、クラウド化による運用負担の軽減やコスト削減を理由とする回答が多い
- 一方で、既存システム環境の制約や機密情報の取扱いなど移行性やセキュリティ観点でクラウドファーストとまでは言えないという回答が多かった

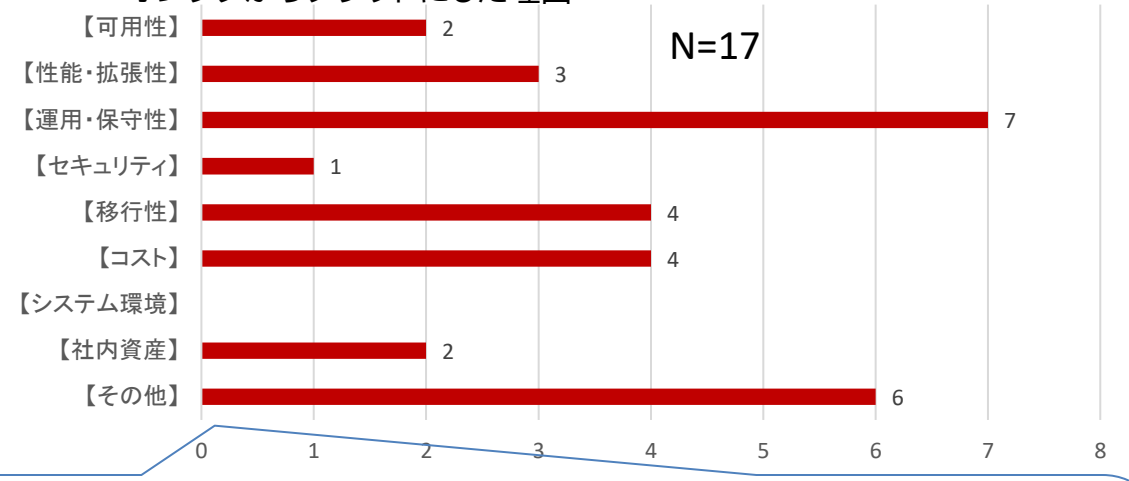
アンケート②:【クラウドファースト】クラウドを選択するシステム・理由

「クラウドファースト方針」の回答者から見えてくる、クラウド化しやすいシステムやクラウド化の理由

Q1　クラウドに既に移行されているシステム又はクラウドで新規構築したシステムはどのようなものがありますか？（複数選択可能）



＜オンプレからクラウドにした理由＞



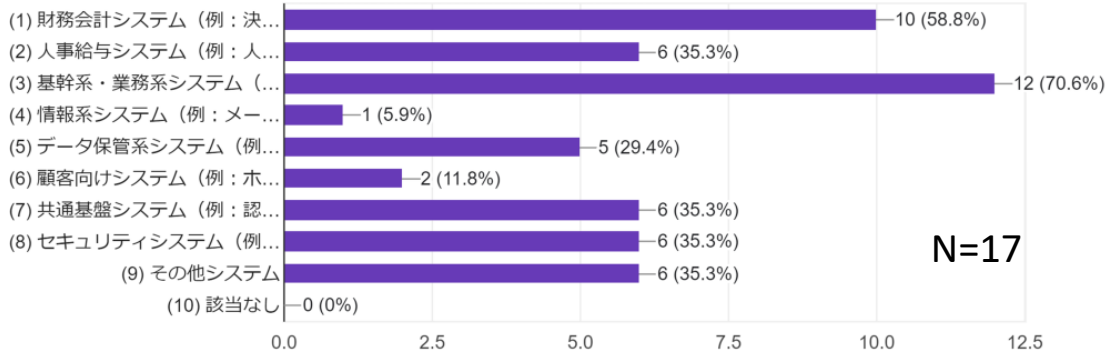
- 運用管理手間・費用を抑制したい【運用・保守性】【コスト】
- SaaS等のシステムが増えてくる中で、認証基盤についてもCloudで活用した方がコスト面、運用管理面でメリットがあるため。【コスト】【運用・保守性】
- さまざまなビジネスニーズに応えていくため。有スキル者確保が不要なため。最新のアプリケーション機能が利用可能なため。導入期間の短縮と運用負荷の低減が図れるため。【性能・拡張性】【社内資産】【移行性】【運用・保守性】
- インフラ環境の構築・維持管理コスト削減、柔軟性・冗長性やマネージドサービスなどパブリッククラウドならではの利便性の享受【可用性】【性能・拡張性】【コスト】　等

- クラウド化したシステムとしては情報系システムなど、移行に踏み切りやすく運用・保守性でメリットの出やすいものが選ばれている傾向
- クラウド化した理由としては、運用・保守性以外に、会社で決められたクラウド化方針に沿う流れといった回答も多く見られた（その他として分類）

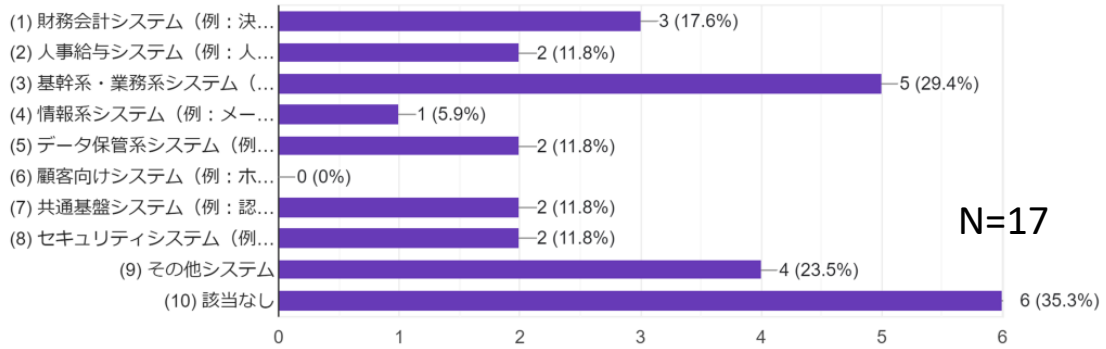
アンケート③:【クラウドファースト】オンプレに残るシステム・理由

「クラウドファースト方針」の回答者から見えてくる、オンプレに残る傾向のシステムやその理由

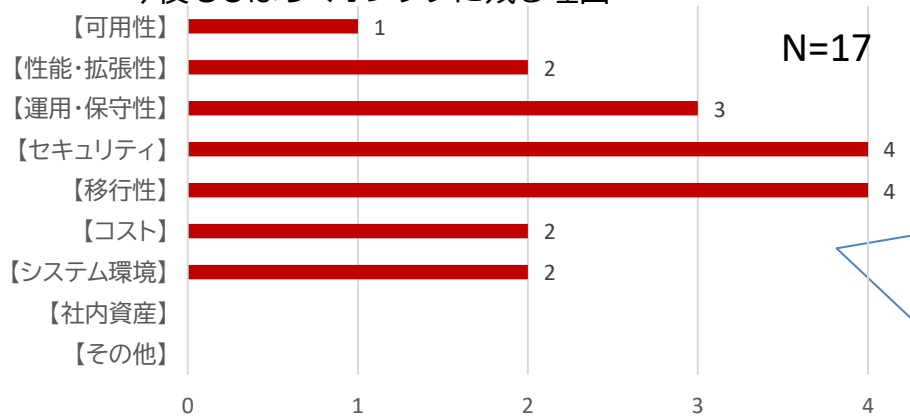
Q2　現時点でオンプレとして残っているシステムはどのようなものがありますか？（複数選択可能）



Q3　今後もしばらくオンプレとして残るシステムはどのようなものがありますか？（複数選択可能）



＜今後もしばらくオンプレに残る理由＞



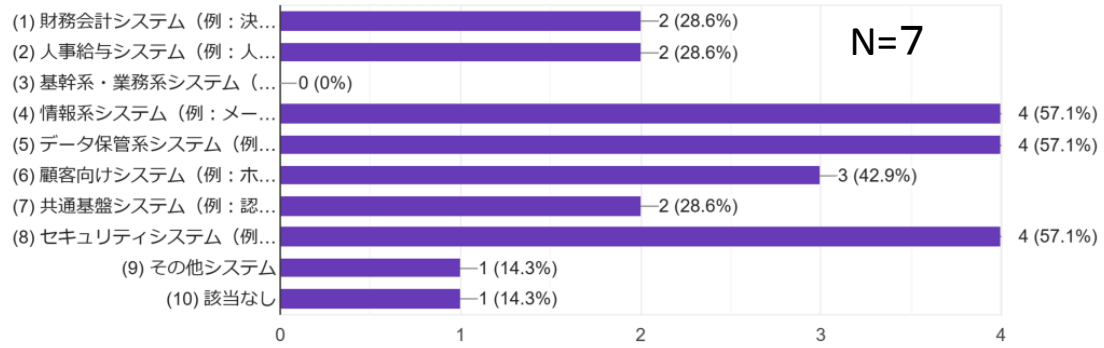
- 検討した結果、メインフレームとのDB接続が性能面と障害対応面で安定しなかったから【性能・拡張性】【運用・保守性】
- クラウド上に置けないデータがあるため。また、オンプレでないと要件を満たせないため。【セキュリティ】
- コア技術情報を保有しており情報流出時のリスクが極大・性能面で特殊仕様を要する・障害時は優先的に復旧が必要など、要件として高可用性がある【セキュリティ】【性能・拡張性】【運用・保守性】【可用性】　等

- 基幹系・業務系システムは、現時点及び今後もオンプレとして残る傾向が強く、セキュリティ、運用・保守性が主な要因と考えられる
- 一方で、今後の観点（Q3）では該当なしの選択も一定数あり、クラウド化に積極的な方向性も見受けられる

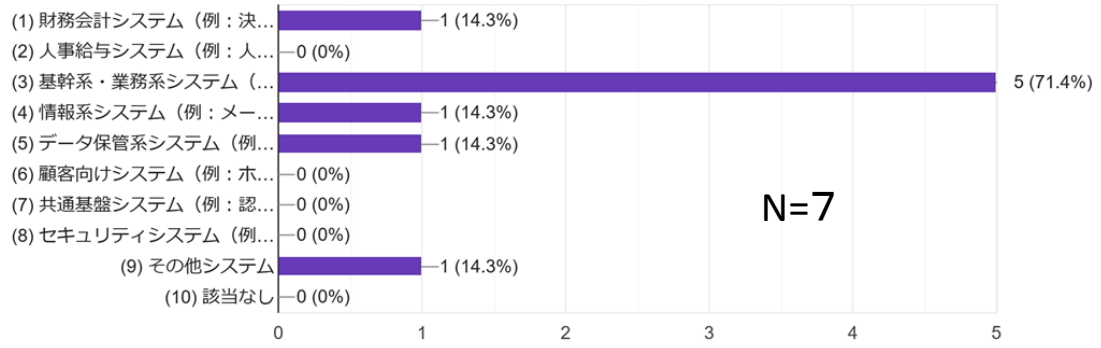
アンケート④：
【クラウドファーストではない】オンプレに残るシステム・理由

「クラウドファーストとまでは言えない」の回答者から見えてくる、クラウド選択するシステムやオンプレに残るシステムとその理由

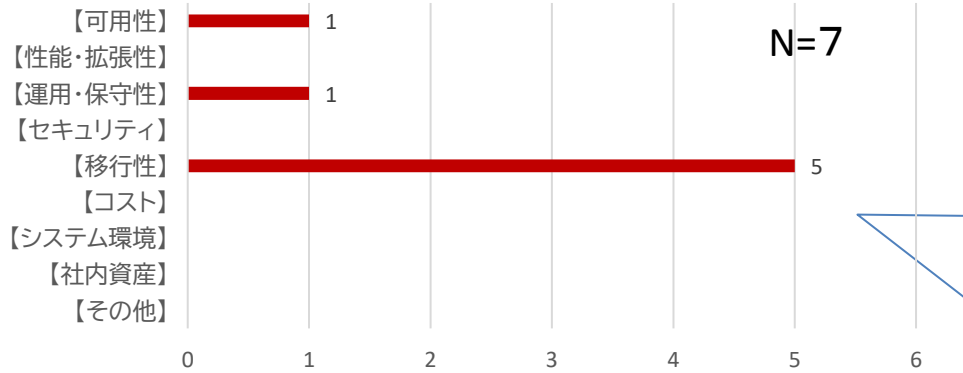
Q4　クラウドで構築しているシステムがあればどのようなシステムですか？（複数選択可能）



Q5　今後もしばらくオンプレとして残るシステムはどのようなものがありますか？（複数選択可能）



＜今後もしばらくオンプレに残る理由＞



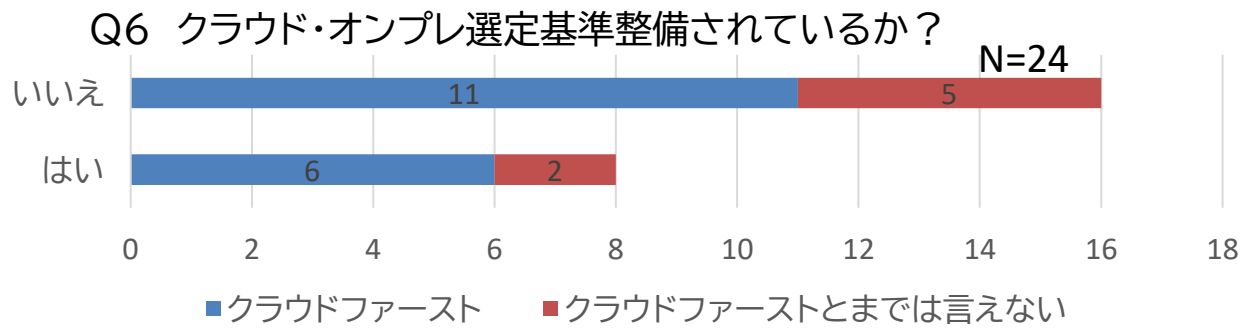
- 社内オンプレによる仮想基盤が充実しており運用体制も盤石であるが故に、現状の環境からの移行を考えていないため。【移行性】
- 方式を変えることで他システムへの影響が大きいことが見込まれるため。【移行性】
- 将来的には工場系のシステムは物理的な機器とのリスポンスの関係によりオンプレを選択することになると予想される。【移行性】　等

- 「クラウドファーストとまでは言えない」の場合でも、基幹系・業務系システムのオンプレ傾向が強く出ており、移行性が主な要因になっている
- 一方で、情報系、データ保管系、セキュリティシステムなどは比較的クラウド化する傾向がみられる

アンケート考察

- 「クラウドファースト方針」と「クラウドファースト方針とまでは言えない」の両方で共通するシステムの**オンプレ傾向**は、**基幹系・業務系システム**となった。
- また、**クラウド化しているシステムの傾向**としては、「クラウドファースト方針」の回答の中では情報系システム、顧客向けシステム、共通基盤システムで、「クラウドファースト方針とまでは言えない」の回答の中では情報系システム、データ保管システム、セキュリティシステムとなり、共通するものは**情報系システム**となった。
- 「クラウドファースト方針」の回答で、クラウド化に期待するところとして**運用・保守性**や**コスト**があがっており、クラウドを積極的に利用することで管理負担や費用を抑えるなどメリットを意識した背景が読み取れる。
- 「クラウドファースト方針」と「クラウドファースト方針とまでは言えない」の回答で共通する**オンプレに残る理由**として**移行性**があり、他システムとの連携や既存システムへの影響度合いなど検討の段階で移行すること自体がネックとなりオンプレに残る傾向がみられる。
- 一方で、**オンプレ傾向の高い基幹系システム**で**オンプレとして残る理由**として**セキュリティ**、**運用・保守性**が入ってくる。

⇒システムの性質をふまえながら環境を選択することが適していると考えられ、より網羅的な観点での評価として**オンプレ・クラウド選定基準を活用**頂きたい。



「はい」の場合でも明確な選定基準についての回答はなかった
⇒今回の選定基準考察が役に立つのでは

システム構築時におけるオンプレ・クラウド選定の判断基準

■ITインフラ研究会参加企業に実施した**アンケートの結果**および分科会1メンバーの**クラウド導入事例**からオンプレ・クラウド選定の判断項目を抽出し、6つの分類に整理

【抽出したオンプレ・クラウド選定の判断項目※一部抜粋】

可用性

- 高い可用性が求められ、クラウド事業者によるメンテナンスなど許容できない部分がある
  →システムの稼働レベル
- ・障害時には優先的に復旧が必要など、要件として高可用性がある
  →BCP対策の実現性

運用・保守性

- 維持管理手間を削減したいため
  →運用負荷の許容度

セキュリティ

- 特定の場所や端末からしか許可されていない業務がある
  →データ管理のユーザ要望や法的規制への影響度

性能・拡張性

- 検討した結果、メインフレームとのDB接続が性能面と障害対応面で安定しなかったから
  →外部とのデータ処理量
- 一時的なアクセス集中によるサーバへの高負荷に柔軟に対応する必要があるため
  →負荷変動性

移行性

- システム導入期間の短縮
  →リリースのスピード感
- 性能面で特殊仕様を要する
  →作り込み度合
  （特殊な要件）

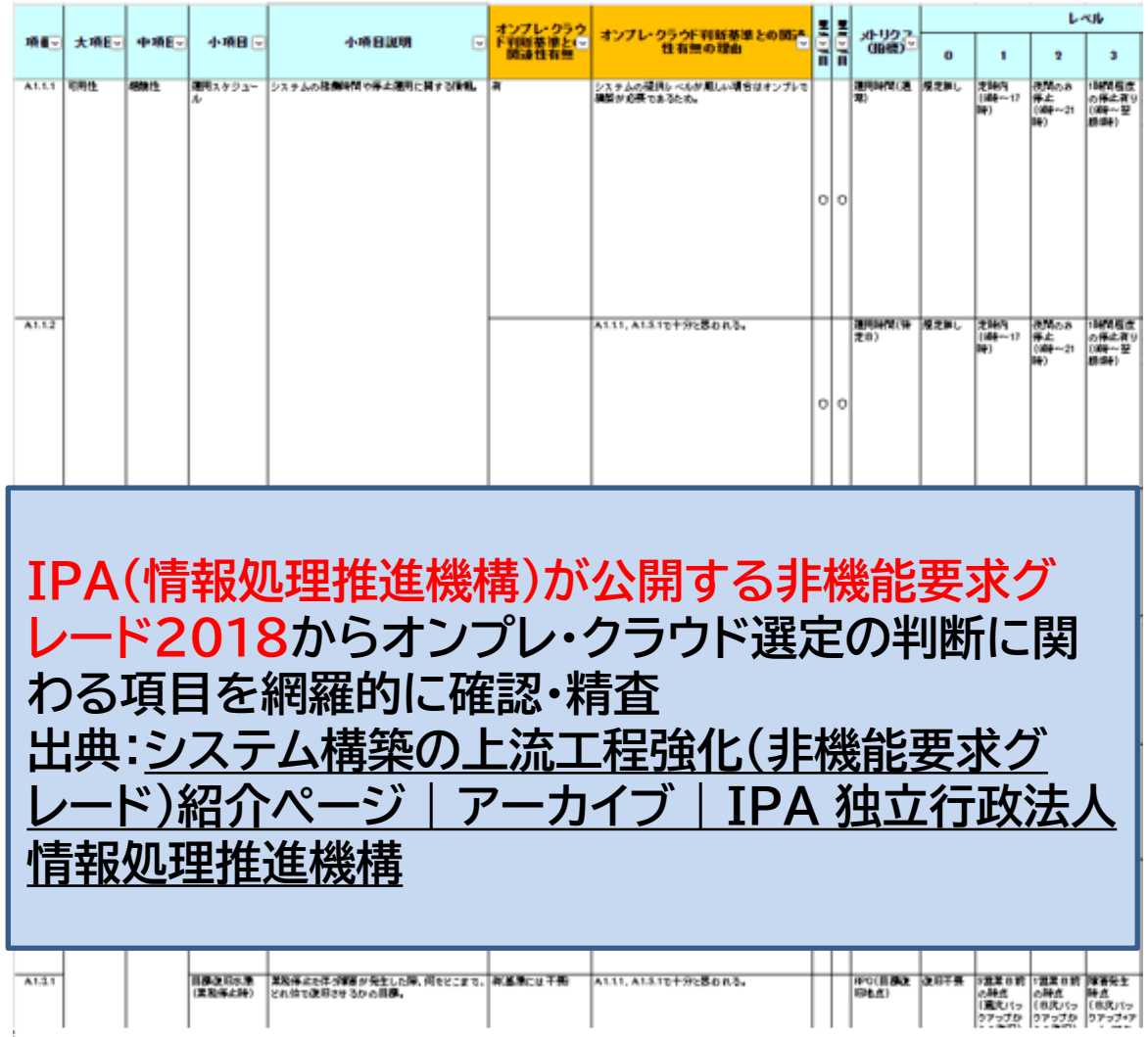
システム環境・エコロジー

- テレワーク、社外コラボ環境の確保
  →社外との協業

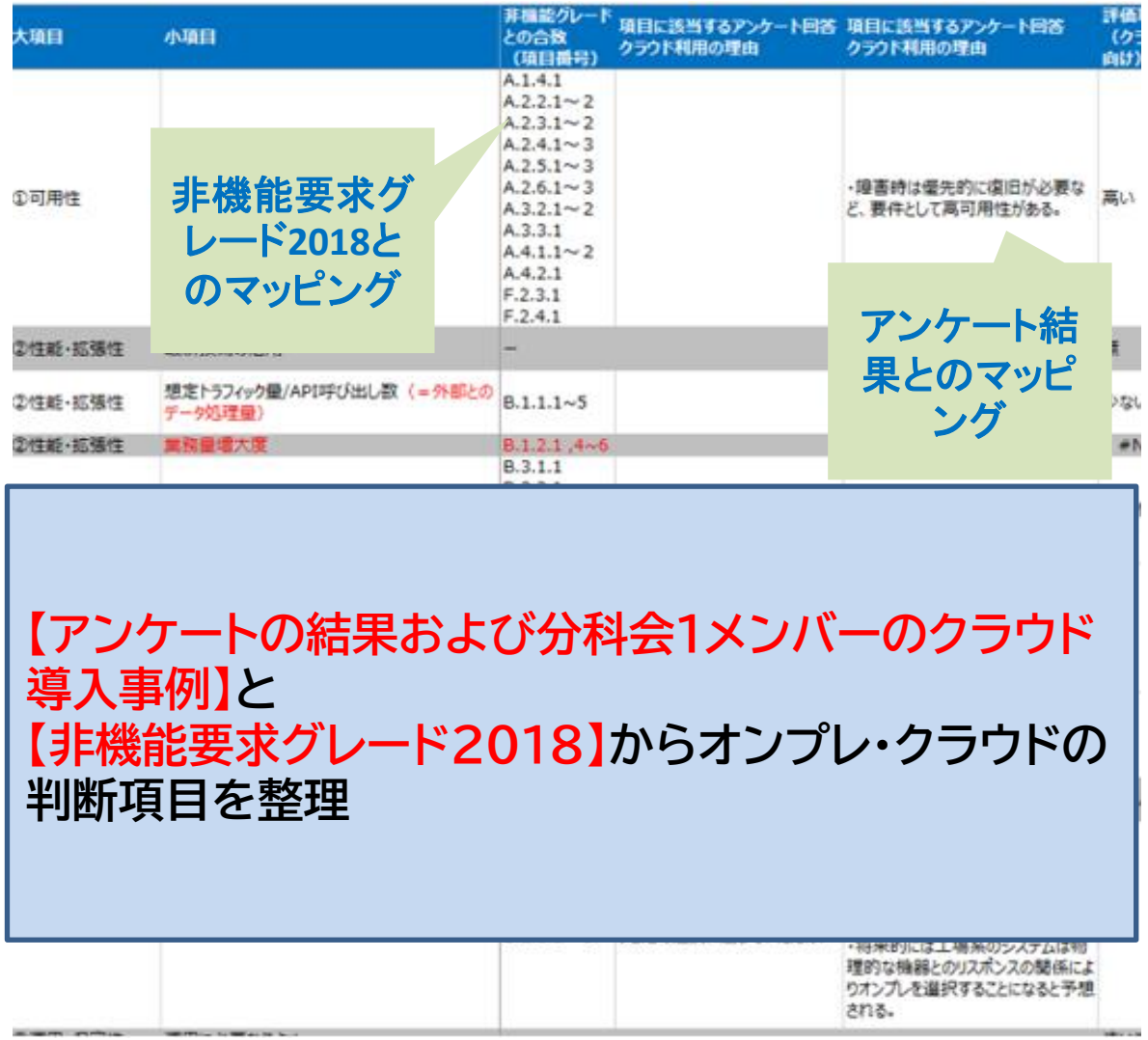
オンプレ・クラウドどちらで構築するか？

など

システム構築時におけるオンプレ・クラウド選定の判断基準

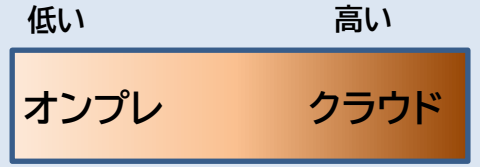


IPA(情報処理推進機構)が公開する非機能要求グレード2018からオンプレ・クラウド選定の判断に関わる項目を網羅的に確認・精査
出典:システム構築の上流工程強化(非機能要求グレード)紹介ページ｜アーカイブ｜IPA 独立行政法人 情報処理推進機構

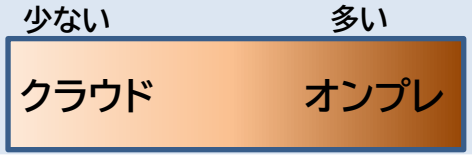
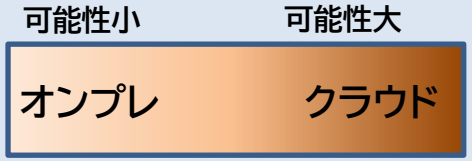
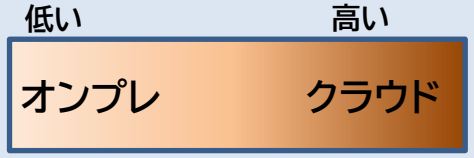
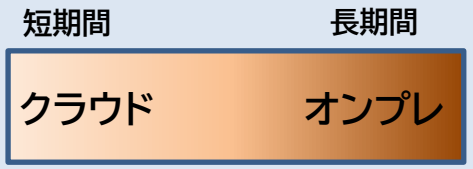
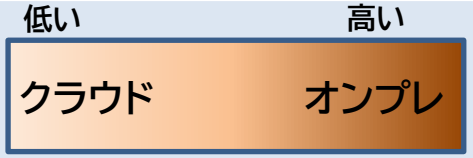


【アンケートの結果および分科会1メンバーのクラウド導入事例】と
【非機能要求グレード2018】からオンプレ・クラウドの判断項目を整理

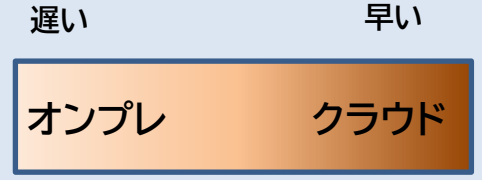
システム構築時におけるオンプレ・クラウド選定の判断基準

項目	補足説明	判断イメージ
①可用性		
システム稼働レベル	クラウドはサービスプロバイダーがある程度のサービスレベルを保証しているため、一般的な利用においては要件を満たせるが、99.999%など非常に高い要求がある場合は企業が物理的にハードウェアとソフトウェアを所有しているオンプレで構築する必要がある。	
BCP対策の実現性	クラウドはコンソール上で利用拠点を指定できるため、複数拠点に分散したシステム構築が容易である。オンプレは複数拠点での構築が容易ではない。	

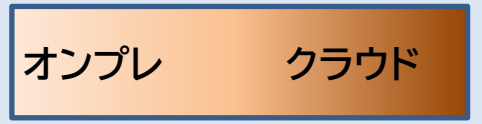
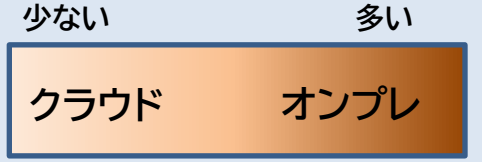
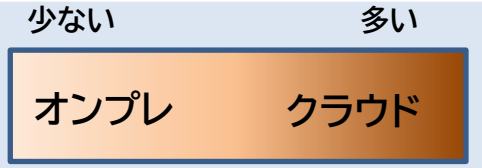
システム構築時におけるオンプレ・クラウド選定の判断基準

項目	補足説明	判断イメージ
②性能・拡張性		
外部とのデータ処理量	クラウドの利用料金は、一般的にインスタンス、ストレージ、データ転送量の利用状況に基づき請求される。データの転送量が多いシステムでは、コストの観点でオンプレの方が優位である。	
システム拡張性	スモールスタートし、段階的にサービス展開の拡大や機能拡張を想定している場合はリソースの拡張が容易という観点からクラウドの方が優位である。	
負荷変動性	リソースの利用量がピーク時とそれ以外で差が大きいシステム(一時的なアクセス集中が発生するWebシステムや、バッチ処理時に大量の処理が必要なシステムなど)では、動的なリソース増強が可能なクラウドの方が優位である。	
③運用・保守性		
システムの想定利用期間	一般的に長期的に使用した場合のトータルコストはクラウドよりオンプレの方が安くなる。システムの長期利用を想定している場合はオンプレの方がコストの観点で優位である。一方で、長期間利用により機器の部材確保が困難となる可能性があるため、保守調整の手間を考慮する必要がある。	
運用負荷の許容度	クラウドは、サービスプロバイダーがサービスを提供し、責任分界点が明確なため、自社の守備範囲が限定される。オンプレは物理機器の交換からシステムのバージョンアップなどサービス全体を自社で管理する必要がある。	

システム構築時におけるオンプレ・クラウド選定の判断基準

項目	補足説明	判断イメージ
④移行性		
作り込み度合 （特殊な機能要件）	オンプレは、企業が物理的なハードウェアとソフトウェアを所有しており、完全な管理権限にて特定の要件やニーズに合わせ細かくカスタマイズすることが可能である。クラウドは、基盤やサービスをクラウドプロバイダーが提供しているため、カスタマイズの範囲はオンプレより制限される。	
開発期間	リリースや機能追加が頻繁に発生するサービスにおいては、拡張性が高いクラウドサービスを利用することで最新機能を利用しやすくなる。 オンプレは機器手配に時間を要する可能性があるが、クラウドでは手配が不要で契約タイミングからコンソールで利用できる。	
保有ライセンスの クラウド適用有無	既存のオンプレで取得したライセンスをクラウド環境で利用できる場合は、新規でライセンスを購入する必要がなく、コストメリットが得られるとともにスムーズな移行が可能である。	
他システムとの データ連携	他システムと密な連携が必要な場合、連携するシステムの設置場所を意識して構築する必要がある。オンプレのシステムと連携し、高いレスポンス性が要求されるシステムをクラウドに移行する場合は通信遅延の観点で連携システムも含めてクラウドへの移行を検討する必要がある。	

システム構築時におけるオンプレ・クラウド選定の判断基準

項目	補足説明	判断イメージ
⑤セキュリティ		
データ管理のユーザ要望や法的規制への影響度	各業界、国・地域ごとに異なる法規制に対応する必要があるが、オンプレの場合は自社で統制することができるが、クラウドの場合はクラウド提供事業者側で統制するため利用者側は決められた運用と安全対策に依存することになるため、法規制へ柔軟に対応しやすいという観点でオンプレのほうが優位である。	
⑥システム環境・エコロジー		
為替による金額変動のリスク受容	代表的なクラウドサービスといえば、Microsoftが提供する「Azure」やAmazonが提供する「AWS」など外資系クラウドが挙げられる。 外資系クラウドでは、ドル建てで利用料を支払うことになるが、為替相場によって円で支払う金額は大きく変動する。為替変動リスクを受け入れることができるかがクラウド選定する上での一つの要因といえる。	
CO2排出量	各クラウド事業者のデータセンターでは電力の最適化に細心の注意を払ってサーバシステムの設計、排出量の情報を確認するサービスを提供しており、また各利用者でリソースを共有することでサーバをより高いレベルで無駄なく利用することができる点でオンプレよりもクラウドに優位性がある。	
社外との協業	社外のパートナーやグループのネットワークに接続していないグループ会社と協業に利用するシステムなどインターネットの世界からアクセスが多いシステムは、イントラ回線への通信量負荷やセキュリティ機能実現の観点からクラウドが優位である。	

まとめ＿分科会1＜オンプレ・クラウド選定基準＞

オンプレ・クラウド選定基準について研究を進め、

①2023年度 ITインフラ研究会参加メンバーへのアンケート（約24名）、

②分科会1メンバーの導入事例（5名）、

③IPA（情報処理推進機構）の非機能要求グレード、

を参考に、オンプレ・クラウド選定基準を**6カテゴリー**（①可用性、②性能・拡張性、③運用・保守性、④移行性、⑤セキュリティ、⑥システム環境・エコロジー）、**15項目**に纏め作成してきた。

オンプレ・クラウド選定基準を策定するにあたり、当初は**点数化**できるツールの作成を目指した。理由としては、点数化することで、（担当者や各社の事情を排除した）より**客観性の高い**判断ツールになると想定したからである。

また一方、実際に検討を進める中で（参加メンバーからのアンケートやメンバーの導入事例などからも）「会社の方針」や「システムの個別事情」がオンプレ・クラウド選定において、**重要**な要素であることを再認識した。そこで、洗い出した項目の**重み付け**の重要性を認識し、点数化にあたっては重み付けも含めた判断基準が望ましいとの結論に至った。

今回策定したオンプレ・クラウド選定基準は、項目の洗い出しまでとはなります。

冒頭資料の通り、2022年時点で約7割の企業がクラウドサービスを利用しており、ITインフラにおいてクラウドは各社共通の取り組みテーマになっています。また、参加メンバーへのアンケートでは、オンプレ・クラウド選定基準が明文化されている企業は見つからなかった。

そんな中で、職域、企業方針、クラウド取り組み状況、が異なる**5名**で、オンプレ・クラウド選定基準について真剣に研究できた事は、**価値ある体験**となりました。

2023年度 ITインフラ研究会
分科会2

ゼロトラストを知ってますか？

2024年4月

分科会2

目次

1. 研究目的

従来のセキュリティ対策は、ファイアウォールやVPNなどの技術により境界を設け、外部リスクから守る方法が一般的だった。近年はCOVID19の流行によるテレワークの拡大やクラウド化、ネットワーク機器の脆弱性、および悪意ある第三者の手法変化に伴い、従来の方法（境界型防御）が通用しなくなってきている。
そこで注目となっているのがゼロトラストである。

- ✓ 従来の「外部は危険」「内部は安全」は通用しなくなっている。
- ✓ 全てのアクセスにセキュリティリスクがあると考える。
- ✓ ゼロトラスト（＝何も信用しない）考えで、ネットワーク構成を設計する必要がある。

本研究会ではゼロトラストとは何者なのか、誰でも分かるように噛み砕いて説明し、
後半では、本研究会内でアンケートを取得し、モデルケースを提案する。

なお、記載内容は分科会2の考察です。

目次

2. ゼロトラストとは

- ゼロトラストの定義として、NIST SP800-207で以下のように記載されている。

ゼロトラストは、ネットワークが侵害されている場合であっても、情報システムやサービスにおいて、各リクエストを正確かつ最小の権限となるようにアクセス判断する際の不確実性を最小化するために設計された概念とアイデアの集合体のことである。
【※NIST SP800-207(原文および日本語訳)より抜粋】

- ゼロトラストの原則はNIST SP800-207で以下のように記載されている。
<NISC7か条>

1. すべてのデータソースとコンピューティングサービスをリソースとみなす。
2. ネットワークの場所に関係なく、すべての通信を保護する。
3. 企業リソースへのアクセスは、セッション単位で付与する。
4. リソースへのアクセスは、クライアントアイデンティティ、アプリケーション/サービス、リクエストする資産の状態、その他の行動属性や環境属性を含めた動的ポリシーにより決定する。
5. すべての資産の整合性とセキュリティ動作を監視し、測定する。
6. すべてのリソースの認証と認可を動的に行い、アクセスが許可される前に厳格に実施する。
7. 資産、ネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、セキュリティ態勢の改善に利用する。

※NIST SP800-207(日本語訳)より抜粋

2. ゼロトラストとは

もうちょい噛み砕くとこんな感じです。

①すべてのデータソースとコンピューティングサービスをリソースとみなす
　⇒PCやサーバーだけでなく、社内システム、クラウドサービス等も含め、リソースとして考える。

②ネットワークの場所に関係なく、全ての通信を保護する
　⇒境界型防御における内側（信頼）と外側（不信）の両方を対象とする。

③企業リソースへのアクセスは、セッション単位で付与する
　⇒一度アクセス許可をセッションは一定時間生きており、利用者に効率良いアクセスであったが、必要最小限の権限として、複数のリソースに跨る権限を設けるべきでない。

④リソースへのアクセスは、クライアントID、アプリケーション要求する資産の状態、その他の行動属性や環境属性を含めた動的ポリシーにより決定する
　⇒IDとPWや証明書などの情報を基にアクセス可否してきたが、それに加え、SWのバージョン、アクセス場所や時間など、アクセスの動的な情報を基に、アクセス可否する。

2. ゼロトラストとは

⑤全ての資産の整合性とセキュリティ動作を監視し、測定する
　⇒アクセス元のデバイスのセキュリティが最新となっているが監視し、必要に応じアップデートや修正の指示をする。
　　また、セキュリティが最新でないデバイスに関しては、アクセスを許可しない場合もある。

⑥全てのリソースの認証と認可を動的に行い、アクセスが許可される前に厳格に実施する
　⇒一度承認された通信や端末は再認証不要で効率化を優先している。一方ゼロトラストでは、実行中の通信においても認証・認可を継続して行うことで信頼性を評価し、必要に応じて再認証を行う。

⑦資産、ネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、セキュリティ態勢の改善に利用する
　⇒各リソースのセキュリティ状況、通信状態、アクセスログなどを収集・分析し、動的ポリシーを最新化する。

やっぱりわからないので、次のスライドで小学生でも理解できるように説明します！

2. ゼロトラストのイメージ（境界型防御）

■境界型防御のイメージとして、公共交通機関（電車）で説明します

境界はここ！

①乗車券購入

個人情報との紐づけはない

②改札口

個人情報との紐づけはなく
乗車券を持っていればOK

③乗車

来た電車に乗るだけで好きなところに移動できる
チェックは特になし

2. ゼロトラストのイメージ（境界型防御）

■セキュリティの観点での問題提起とその解決策を以下に記載します

①乗車券購入

②改札口

個人情報との紐づけはなく
乗車券を持っていればOK

問題
買った本人でなくても、通過できる
不正な乗車券の可能性
解決策
買った本人か確認する
不正な乗車券かチェックする

③乗車

来た電車に乗るだけで好きなところに移動できる

改札口を通らずにホームに行ける、電車に乗れる

問題
目的地に向かわない電車も乗れる
乗車券なくても乗れる
解決策
乗車直前/乗車中に乗車券をチェックする
不審な行動をしていないかチェックする

2. ゼロトラストのイメージ

■ゼロトラストのイメージとして、飛行機で羽田空港からダニエル・K・イノウエ(旧ホノルル)空港へ旅行で行くとします。

①搭乗券購入

クレジットカードやパスポート情報
等で本人情報を登録
搭乗券を購入し、飛行機に乗る権利を得る

②羽田空港に行く

電車・バス・自家用車等で向かう

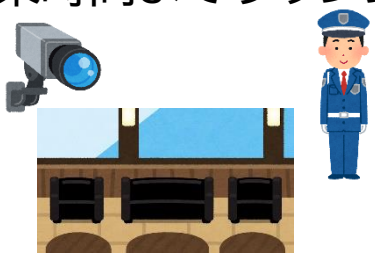
③チェックイン

搭乗券、パスポート等で確認し
搭乗手続きを行う

④手荷物検査

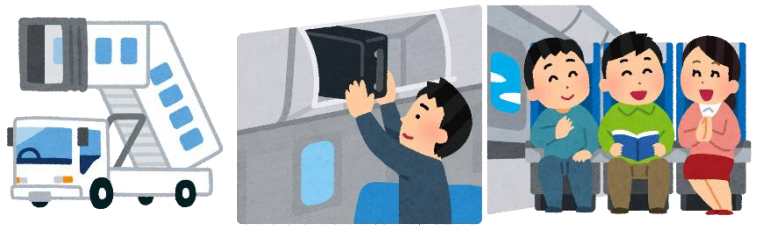
持ち込み禁止物がないか確認
搭乗券などで本人確認

⑤搭乗時間までラウンジで待つ



搭乗時間までラウンジで待つ
監視カメラとか警備員とかも見守り中

⑥搭乗する



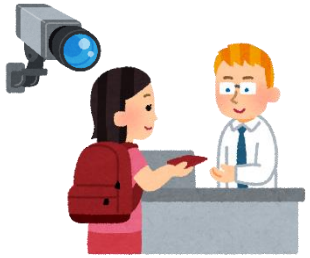
指定された方法で搭乗し、手荷物を入れ
指定された席へ座る

2. ゼロトラストのイメージ

■ゼロトラストのイメージとして、飛行機で羽田空港からダニエル・K・イノウエ(旧ホノルル)空港へ旅行で行くとします。

⑦ダニエル・K・イノウエ空港到着

⑧入国審査



パスポート・ビザ
入国目的等を確認

⑨荷物受取

預けた荷物を受け取る
麻薬探知犬や、警備員が見てる

⑩ハワイの夕日見られたね！

2. ゼロトラストの原則と飛行機の搭乗

■ゼロトラストの原則を飛行機に乗るときの対応例と当てはめると以下のようになる

ゼロトラストの原則	飛行機に乗るときの対応例
1.すべてのデータソースとコンピューティングサービスをリソースとみなす。	旅客だけではなく、乗務員や荷物なども全て管理する。
2. ネットワークの場所に関係なく、すべての通信を保護する。	第三者に中身を見られないように、荷物にロックをかけて預ける。
3. 企業リソースへのアクセスは、セッション単位で付与する。	搭乗ゲートなどの本人確認は大人、子供関係なく全員に対して行う。
4. リソースへのアクセスは、クライアントアイデンティティ、アプリケーション/サービス、リクエストする資産の状態、その他の行動属性や環境属性を含めた動的ポリシーにより決定する。	搭乗ゲートなどの本人確認は搭乗券の内容（期限、性別等）と旅客を照らし合わせて行う。
5. すべての資産の整合性とセキュリティ動作を監視し、測定する。	パスポートや搭乗券に記載されている内容と旅客自身に齟齬がないか確認する。不審な点があれば別室でチェックする。
6. すべてのリソースの認証と認可を動的に行い、アクセスが許可される前に厳格に実施する。	搭乗ゲートではフライトの状況や予約状況と航空券の内容をシステムでチェックする。
7. 資産、ネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、セキュリティ態勢の改善に利用する。	空港内では監視カメラや警備員によって不審者や不審物がないか常に確認する。

2. ゼロトラストの構成要素

ゼロトラストの基本概念に基づくポイントとして、以下の4点を念頭に置く必要がある。
①認証・認可／②クラウド利用／③デバイスセキュリティ／④ログ管理(ログの可視化)

また、その分類として、下記11点がある。
※IPA「ゼロトラスト導入指南書/2021年」参照

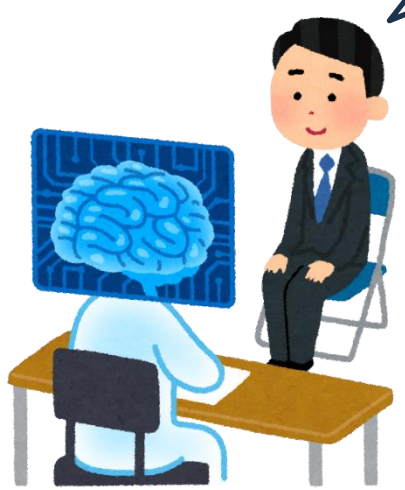
① CASB (Cloud Access Security Broker)
② CSPM (Cloud Security Posture Management)
③ EDR (Endpoint Detection and Response)
④ EMM (Enterprise Mobility Management)
⑤ IDaaS (Identity as a Service)

⇒何が必要なのかわからないので、世の中で話題になっている、「Chat GPT4.0」に意見を求める！

⑩ SOAR (Security Orchestration, Automation and Response)
⑪ UEBA (User and Entity Behavior Analytics)

2. ゼロトラストの構成要素

Q. 最低限のゼロトラストとは？



A. 以下3要素になります。
①マイクロセグメンテーション
②MFA認証
③ログ分析と監視

⇒「マイクロセグメンテーション」「MFA認証」「ログ分析と監視」
を実装できれば、ゼロトラストを名乗ってよい！　と(当分科会では)考える

2. 最小限のゼロトラストとは・・・

分かりやすく分類すると・・・

マイクロセグメンテーション

- SASE
- CASB
- SWG
- CSPM
- SDP

MFA認証

- IDaaS
- IAM

ログ分析・監視

- SIEM
- SOAR
- UEBA

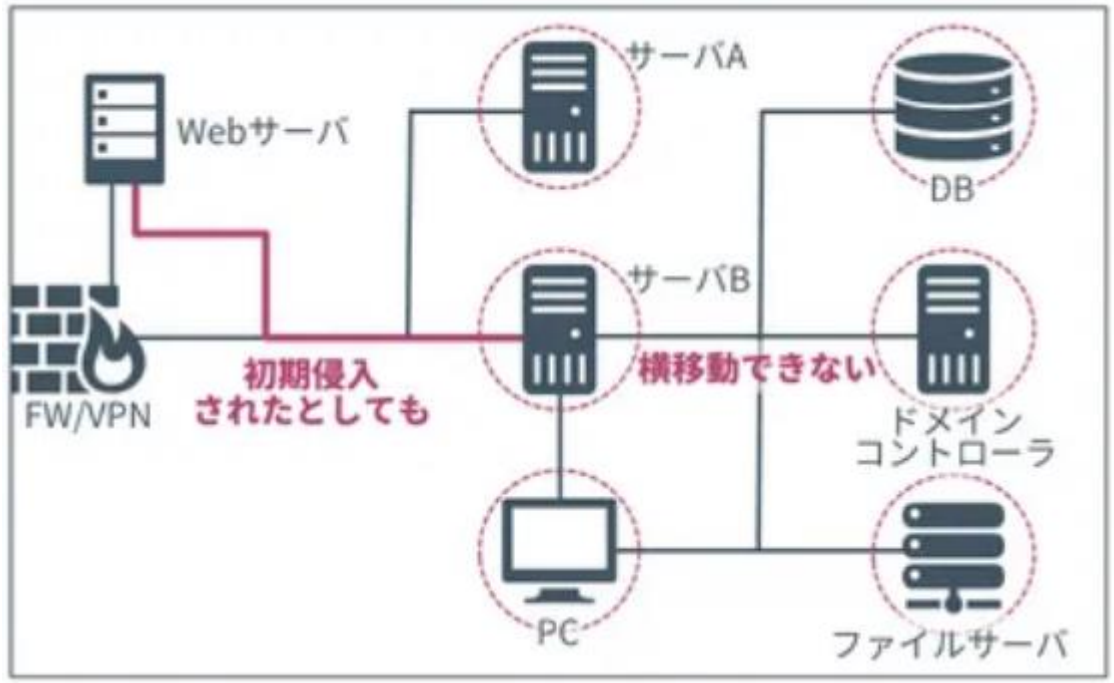
デバイスセキュリティ

- EDR
- EMM

2. 最小限のゼロトラストとは・・・

1. マイクロセグメンテーション

- 従来のファイアウォール等の境界防御ではなく、ホスト単位で論理的な境界を設けることで攻撃の被害を極小化させる。



空港に例えると、保安室、待機スペース、搭乗ゲート等の各部屋に分け、それぞれの通過で搭乗券を提示させることで危険人物が空港内歩き回ることを防ぐ

2. 最小限のゼロトラストとは・・・

2. MFA認証

- 一つの認証で許可させず、複数のステップを踏ませることで
  安全性の担保とする（顔認証＋パスワード、メールアドレス＋秘密の質問）

空港に例えると、搭乗券＋パスポートや、搭乗券＋アプリのQRコードなどで搭乗確認を実施することで本人以外の搭乗を防ぐ

2. 最小限のゼロトラストとは・・・

3. ログ分析と監視

- 機器やシステムからログを収集・分析することで不審や通信の遮断やインシデント時の影響範囲調査に役立てる。

空港に例えると、各スペースに監視カメラを設置して利用者の監視をすることで不審人物を特定する。

目次

3. アンケート概要

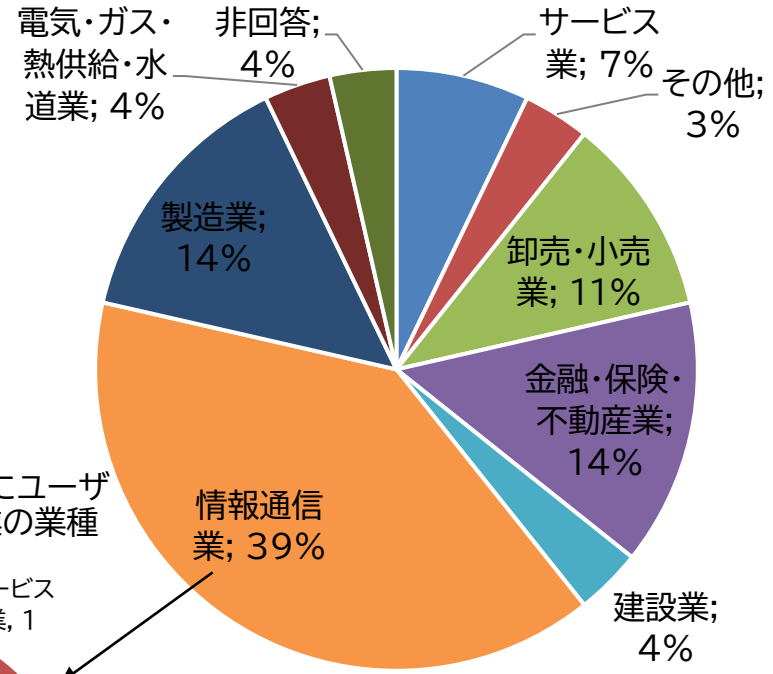
- 目的：ゼロトラスト実装のモデルケースを立案するため、研究会参加企業各社の実装状況についてヒアリングする
- 調査方法：アンケート方式（Microsoft Formsアンケート機能利用）
- 調査期間：2023年12月8日～12月31日
- 調査対象：2023年度ITインフラ研究会参加メンバー（＋幹事団）28名回答
- 調査内容：

1. 業種・規模
2. ゼロトラストの認知度（知らない/概要は分かる/説明できる/提案できる）
3. ゼロトラスト導入状況（全面実装・一部実装・検討中等）
4. ユースケース
   - 主なNW構成（オンプレ・クラウド・ハイブリッドクラウド・マルチクラウド）
   - 利用端末（FAT/シンクラ/スマートデバイス/BYOD）
   - 特定の拠点・端末・人にアクセス限定される業務有無
5. ゼロトラスト実装状況（認証・認可/NW/エンドポイント/ログ取得・分析）
6. その他（フリーコメント）

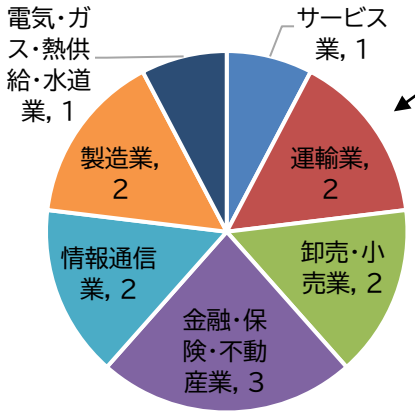
目次

4. アンケート結果① 業種・規模

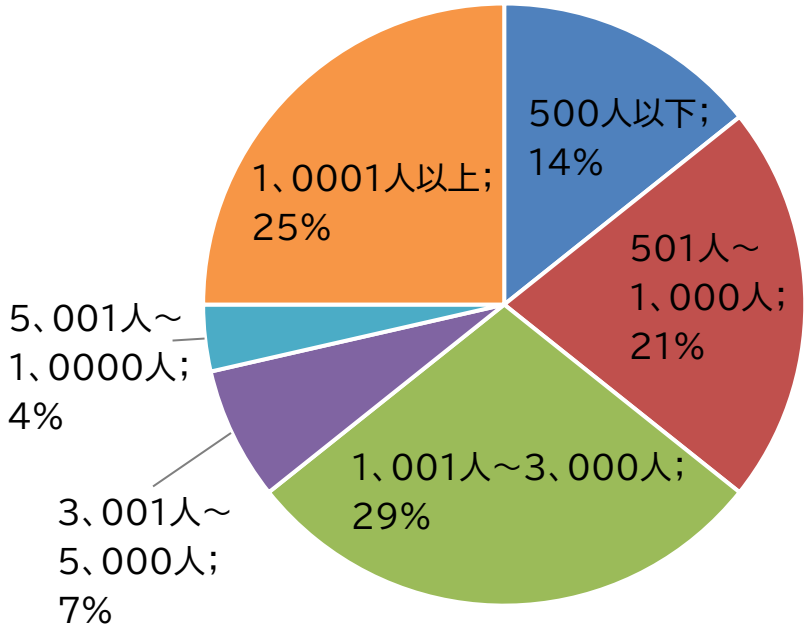
勤務先の業種 (n=28)



(情シス会社で同グループ内にユーザ企業がいる場合)ユーザ企業の業種



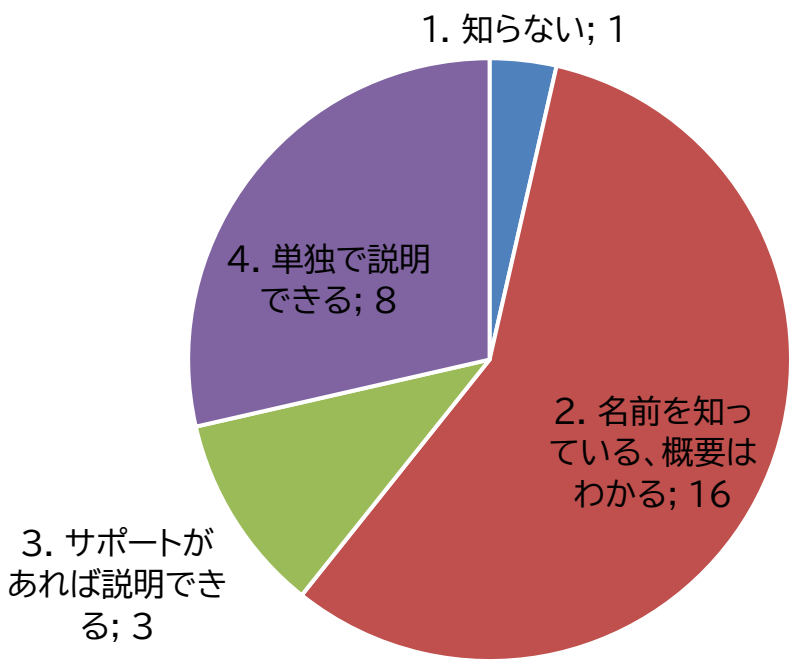
勤務先の従業員数規模 (n=28)



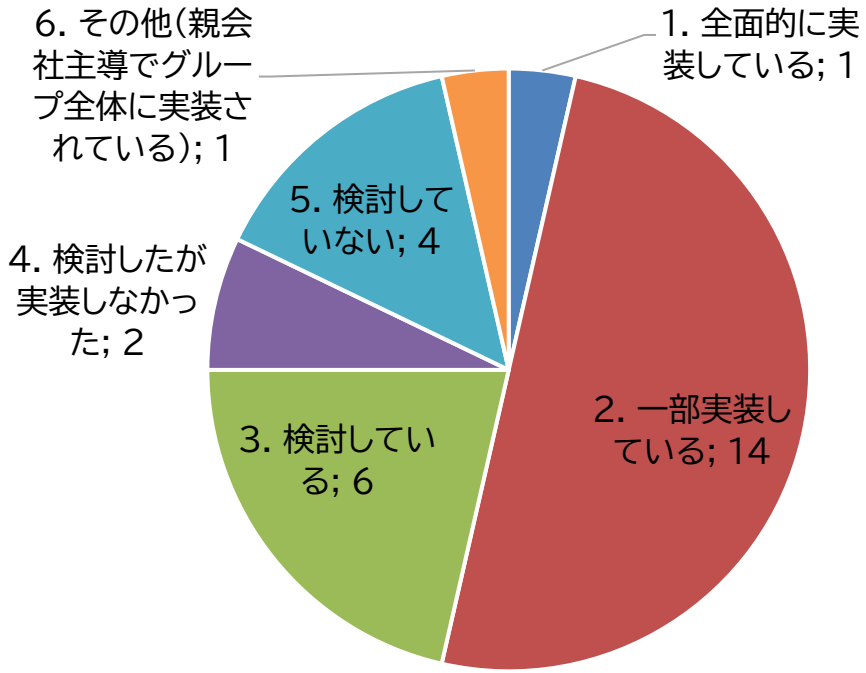
■ 情報通信業を中心として様々な業種・規模の企業が研究会に参加

4. アンケート結果② 認知度・導入状況

ゼロトラストの認知度



ゼロトラストの導入状況



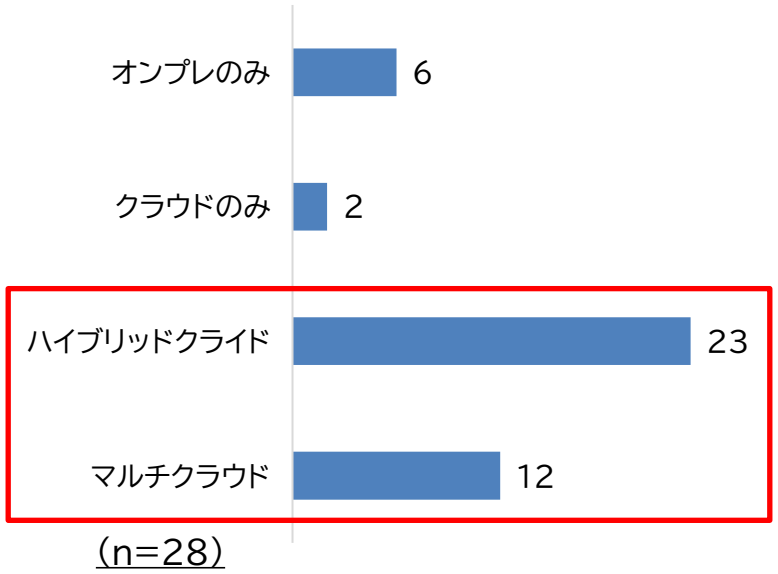
- (サポートがあれば)説明できる研究会参加者は全体の約4割
- 75%の研究会参加企業がゼロトラストを一部実装or検討中

※国内企業は約5割、国内DX認定企業は約9割がゼロトラストを一部実装or検討中
(NRI Secure Insight 2022より)

4. アンケート結果③ ユースケース

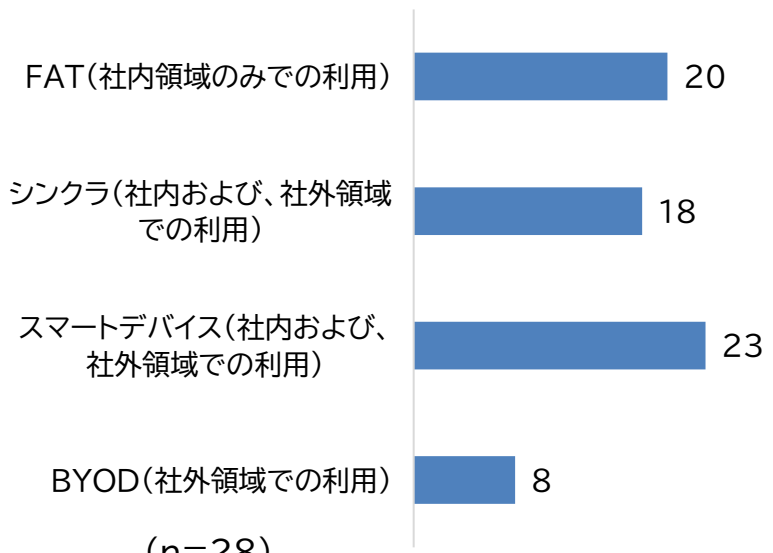
※複数回答可

主なシステムのネットワーク構成



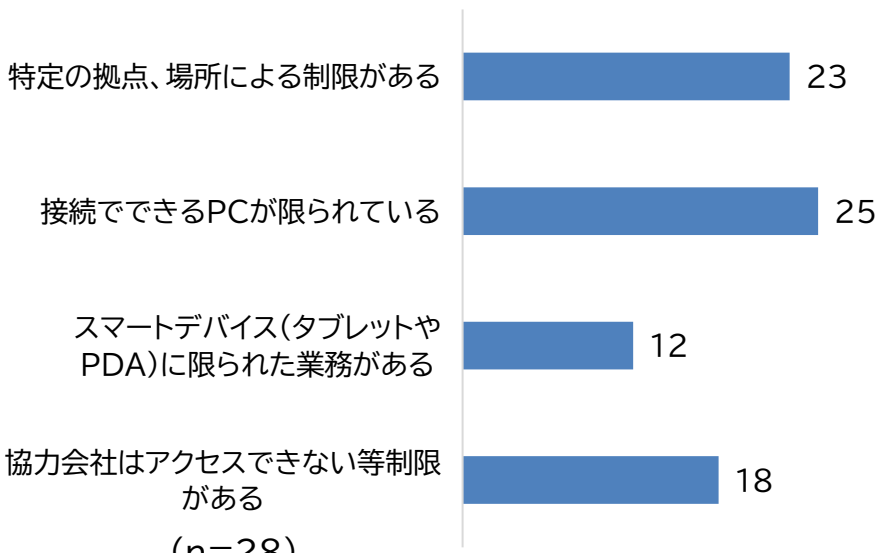
(n=28)

利用端末



(n=28)

特定の拠点・端末・人にアクセス限定される業務の有無



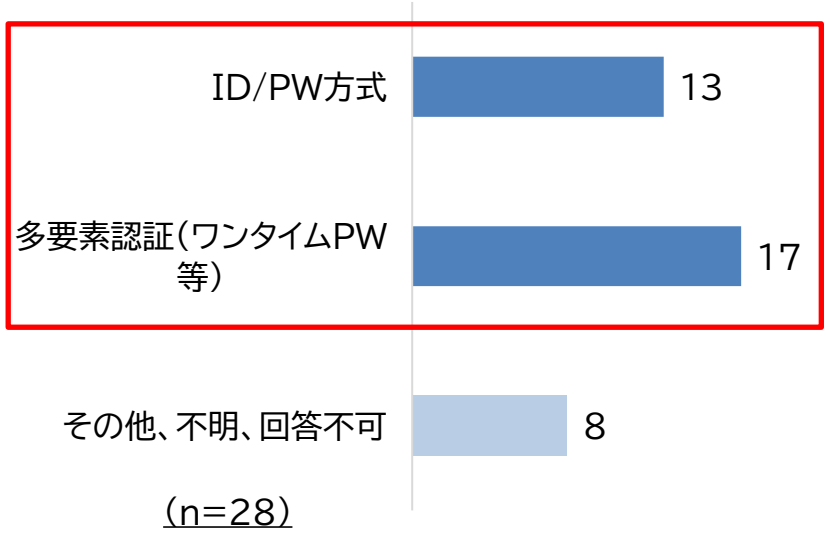
(n=28)

- NW構成：ハイブリットクラウドが半数以上、次点でマルチクラウド　※オンプレ、クラウド単体は少数
- 利用端末：FAT、シンクラ、スマートデバイス、BYODが満遍なく利用されている
- アクセス制御：特定の拠点、端末等で何かしらのアクセス制御をしているところが多い

4. アンケート結果④ ゼロトラスト実装状況(認証・認可)

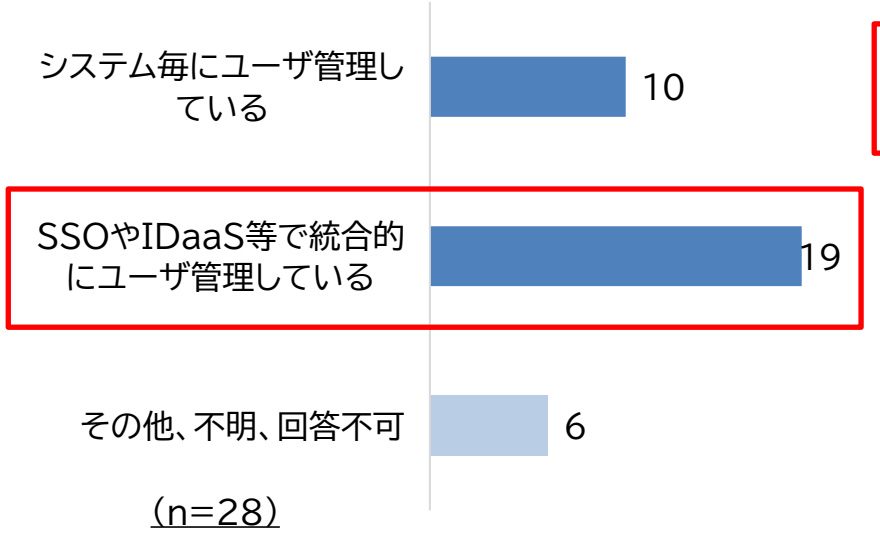
※複数回答可

認証方式



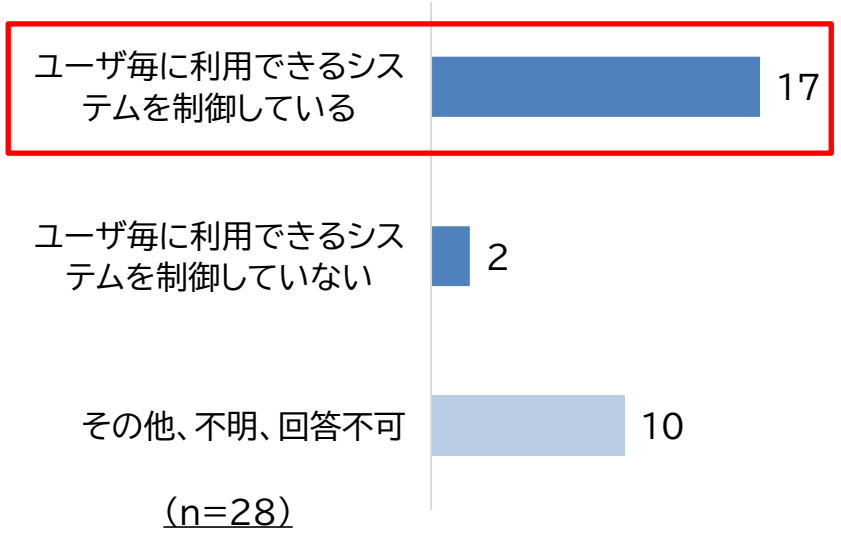
(n=28)

ユーザ管理方式



(n=28)

利用可能システムの制御状況

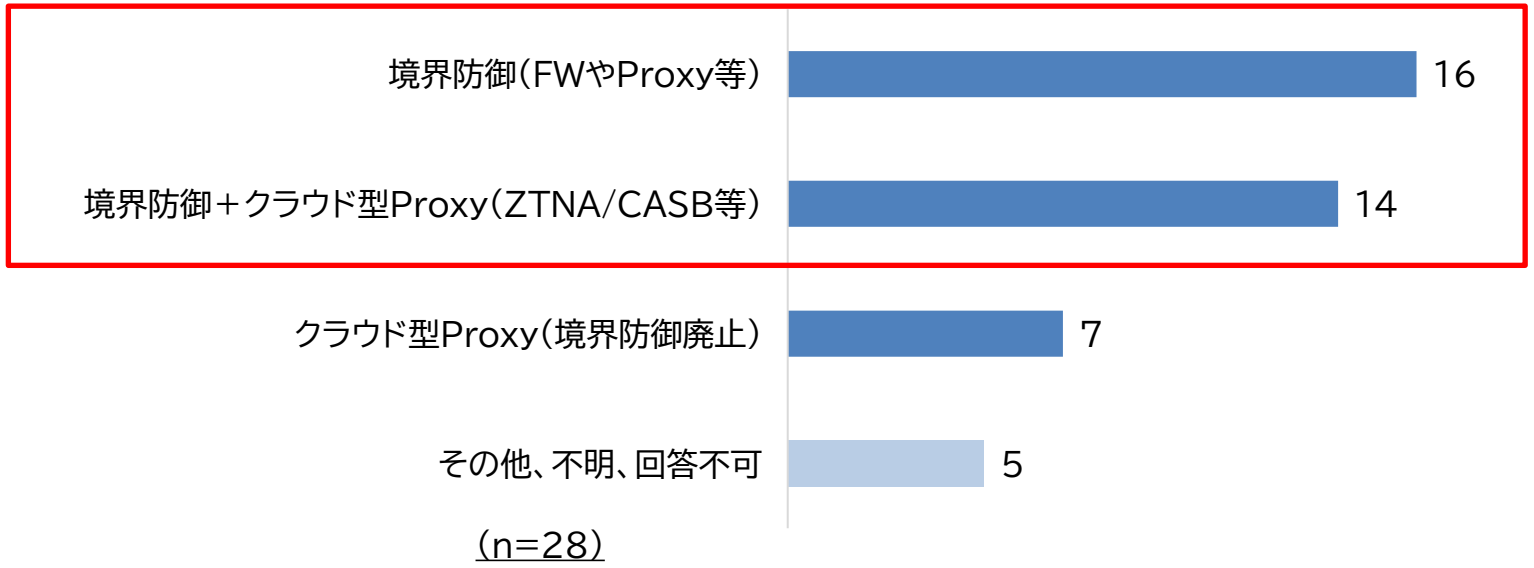


(n=28)

- 回答者の多数がID/PW方式による認証および多要素認証を導入
- ユーザ管理方式は統合的に管理している回答者が多く、次点でシステム毎の管理
- 回答者の多数がユーザ毎に利用可能システムを制限

4. アンケート結果⑤ ゼロトラスト実装状況(ネットワーク)

※複数回答可

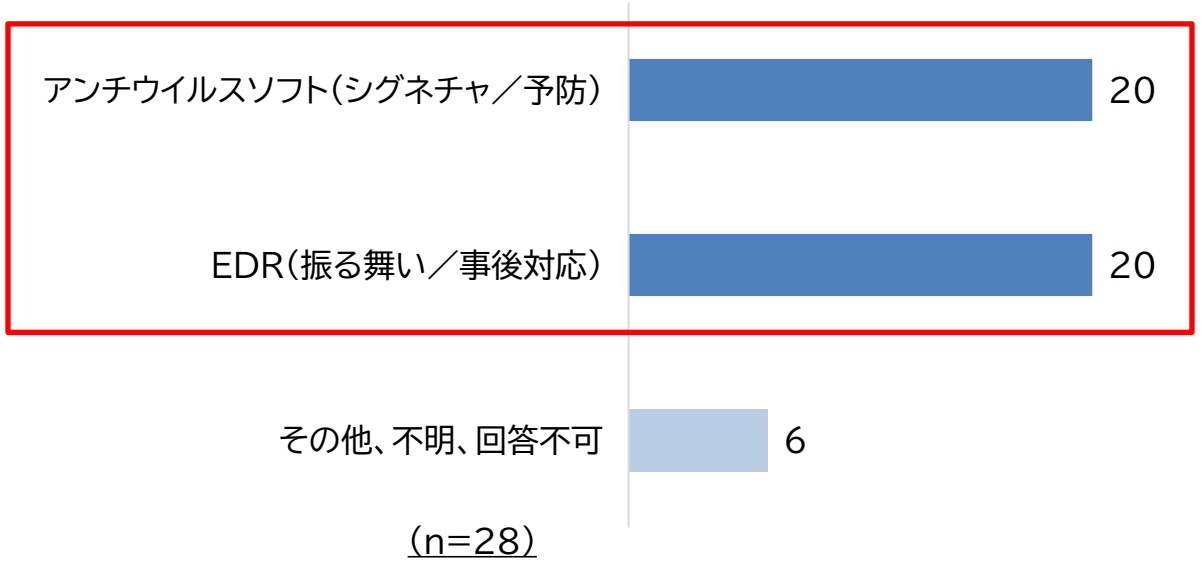


境界防御(FW/Proxy)とクラウド型Proxy(ZTNA/CASB)が多い
※境界防御単体は5名、クラウド型Proxy単体は1名

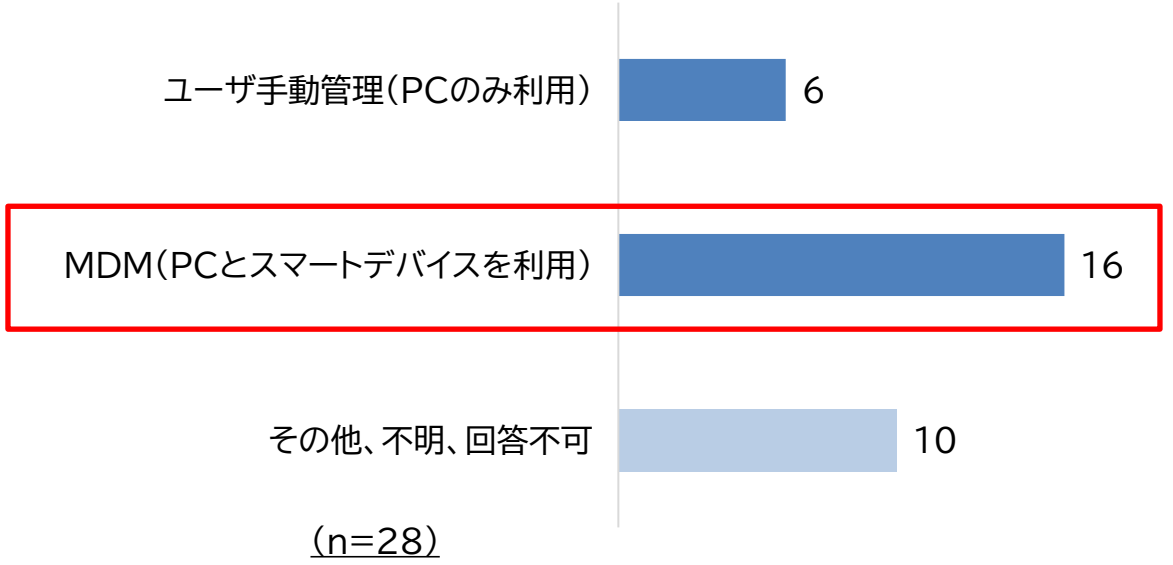
4. アンケート結果⑥ ゼロトラスト実装状況(エンドポイント)

※複数回答可

エンドポイント(マルウェア)



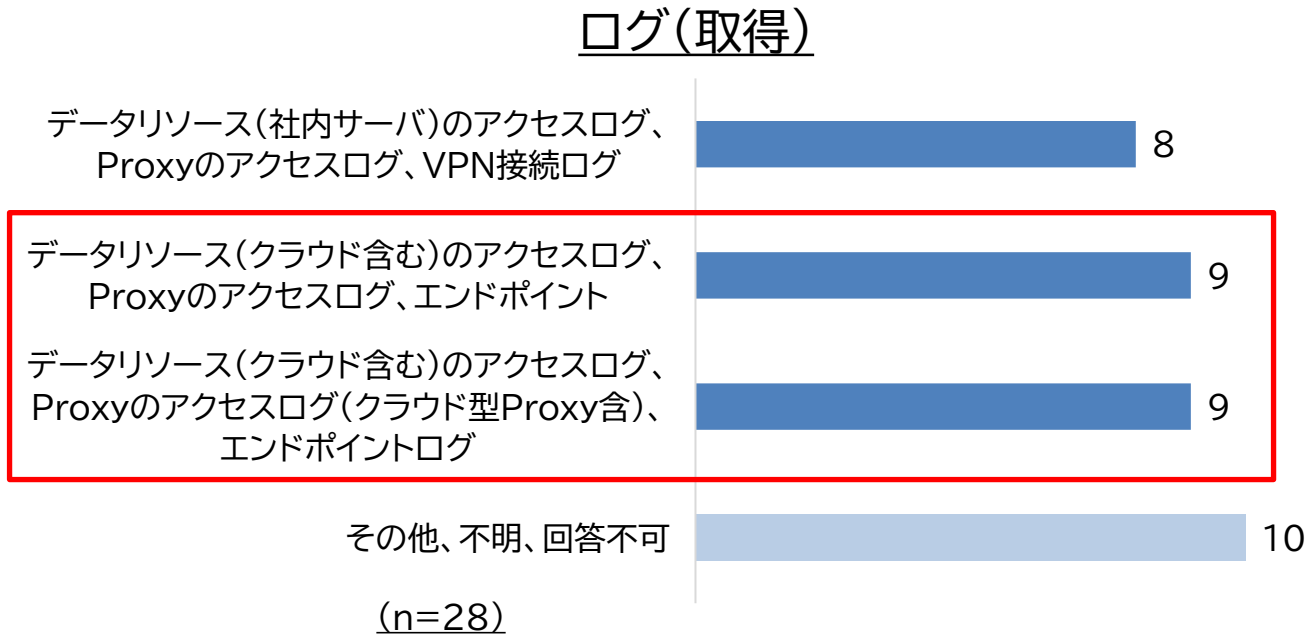
エンドポイント(パッチ・脆弱性)

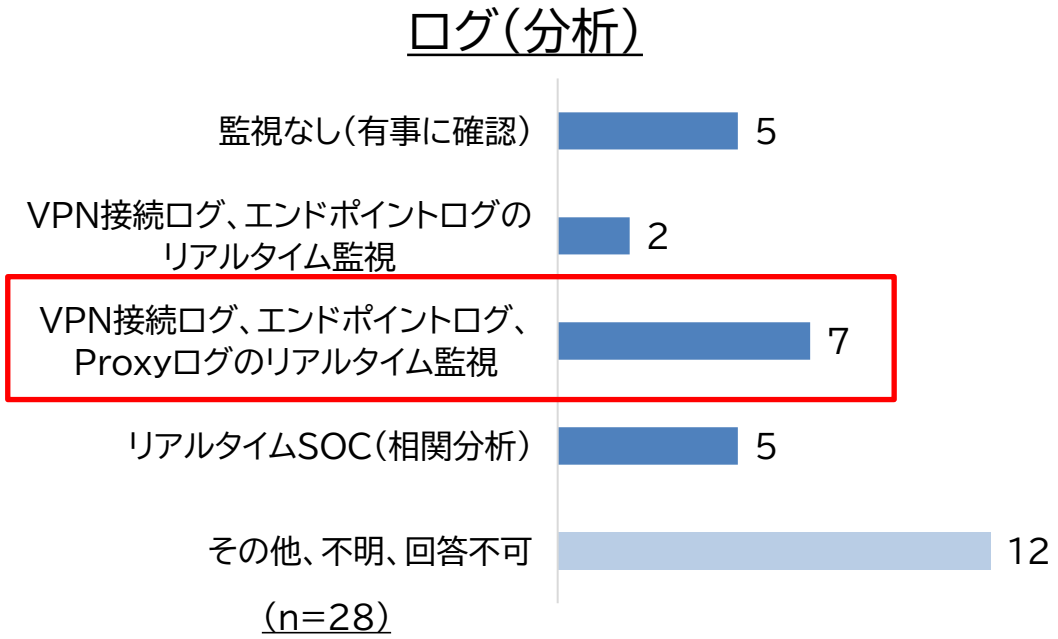


- 回答者の多数がアンチウイルスソフトかEDRを導入、ほとんどは両方実装と回答
- 回答者の多数がMDMを利用して端末管理を実施 (※一部がユーザ手動管理)

4. アンケート結果⑦ ゼロトラスト実装状況(ログ)

※複数回答可





- ログ取得項目は「データリソース(クラウド含む)のアクセスログ、Proxyのアクセスログ、エンドポイント」が多い
- 監視項目は「VPN接続ログ、エンドポイントログ、Proxyログのリアルタイム監視」が多い
  ※リアルタイムSOCもある程度存在
- 有事のみの監視体制も一定数存在

4. アンケートのまとめ

1. ゼロトラストの認知度・導入状況

- (サポートがあれば)ゼロトラストを説明できる参加企業は約4割
- 75%の参加企業がゼロトラストを一部実装or検討中

2. ユースケース、実装状況

- 構成:ハイブリッドクラウド・マルチクラウド環境が多い
- 利用端末: FAT、シンクラ、スマートデバイス、BYODを満遍なく利用
- NW:境界防御(FW/Proxy)とクラウド型Proxy(ZTNA/CASB)が多い
- 認証・認可:多数がID/PW方式や多要素認証、IDaaSやSSO等の統合管理基盤を導入
- エンドポイント:回答者の過半がアンチウイルスソフト+EDRを実装済み
- ログ: 取得項目は「データリソース(クラウド含む)・Proxyのアクセスログ、エンドポイント」、
  監視項目は「VPN接続ログ、エンドポイントログ、Proxyログのリアルタイム監視」が多い

目次

5. モデルケース概要

■研究会参加企業へのアンケートから、各社の実装状況および環境調査を実施。
得られた結果からゼロトラスト導入の参考となるモデルケースを提供
※最小限要素による構成と＋αの2パターンを作成

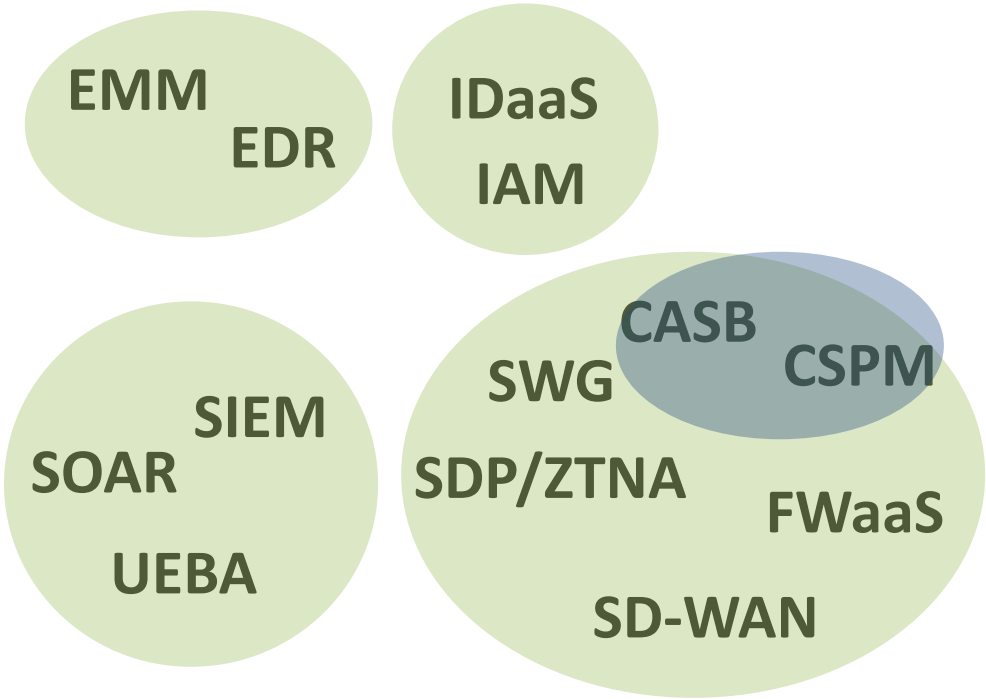
各社の実装状況
導入する環境

モデルケース案

5. モデルケース概要(最小限要素)

■ゼロトラスト構成要素のうち、前項でChat GPTが示した下記要素を含む構成を最小構成とする。

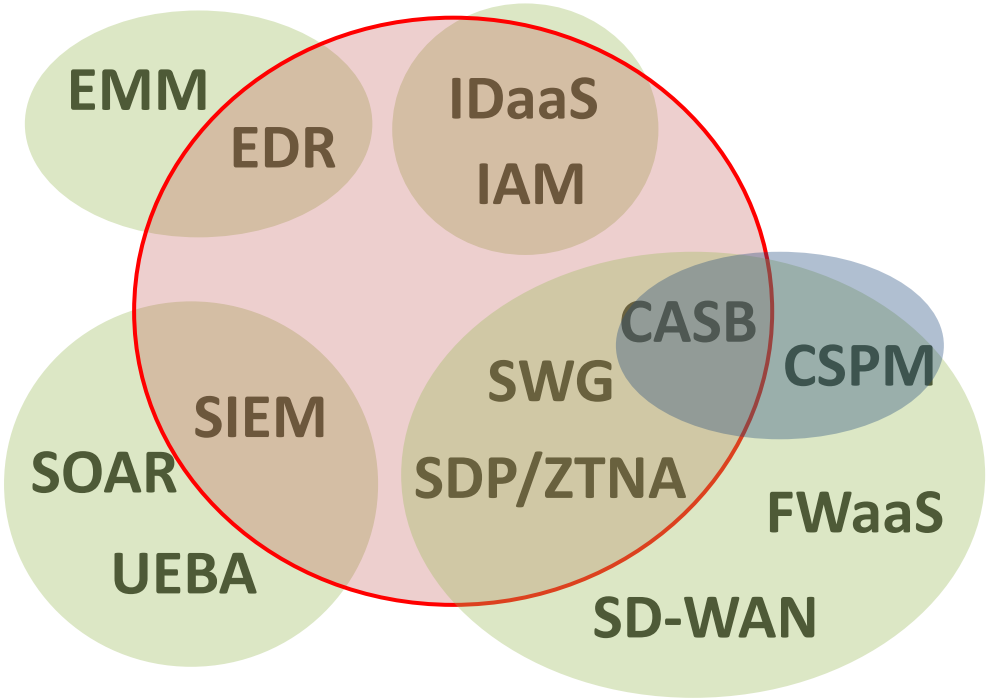
※「デバイスセキュリティ」については最小要素に含まれていないが、アンケートにて過半が実装しているため最小構成に含めて作成



5. モデルケース概要(最小限要素)

■ゼロトラスト構成要素のうち、前項でChat GPTが示した下記要素を含む構成を最小構成とする。

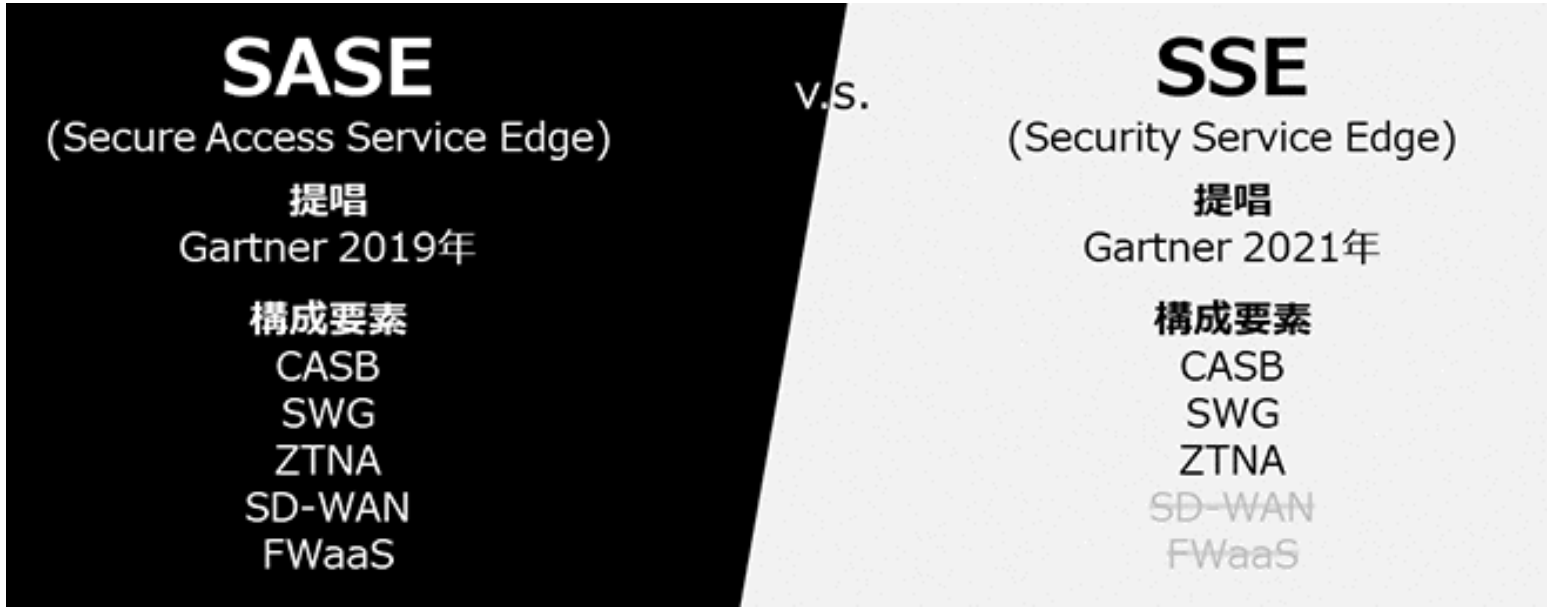
※「デバイスセキュリティ」については最小要素に含まれていないが、アンケートにて過半が実装しているため最小構成に含めて作成



【参考資料】SASEの優先度について（ガートナー社）

■「SASE」を提唱した米ガートナー社は、2021年(※1)にSASEを構成する要素のうち、「CASB」、「SWG」、「ZTNA」の3要素に絞って導入する企業が増えることを予測。
これら基本的な3要素を「SSE」(※2)として提唱している。

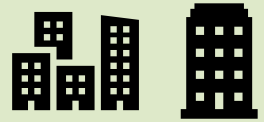
(※1)「2021 Strategic Roadmap for Convergence」
(※2)「Security Service Edge」



5. モデルケース概要(想定環境)

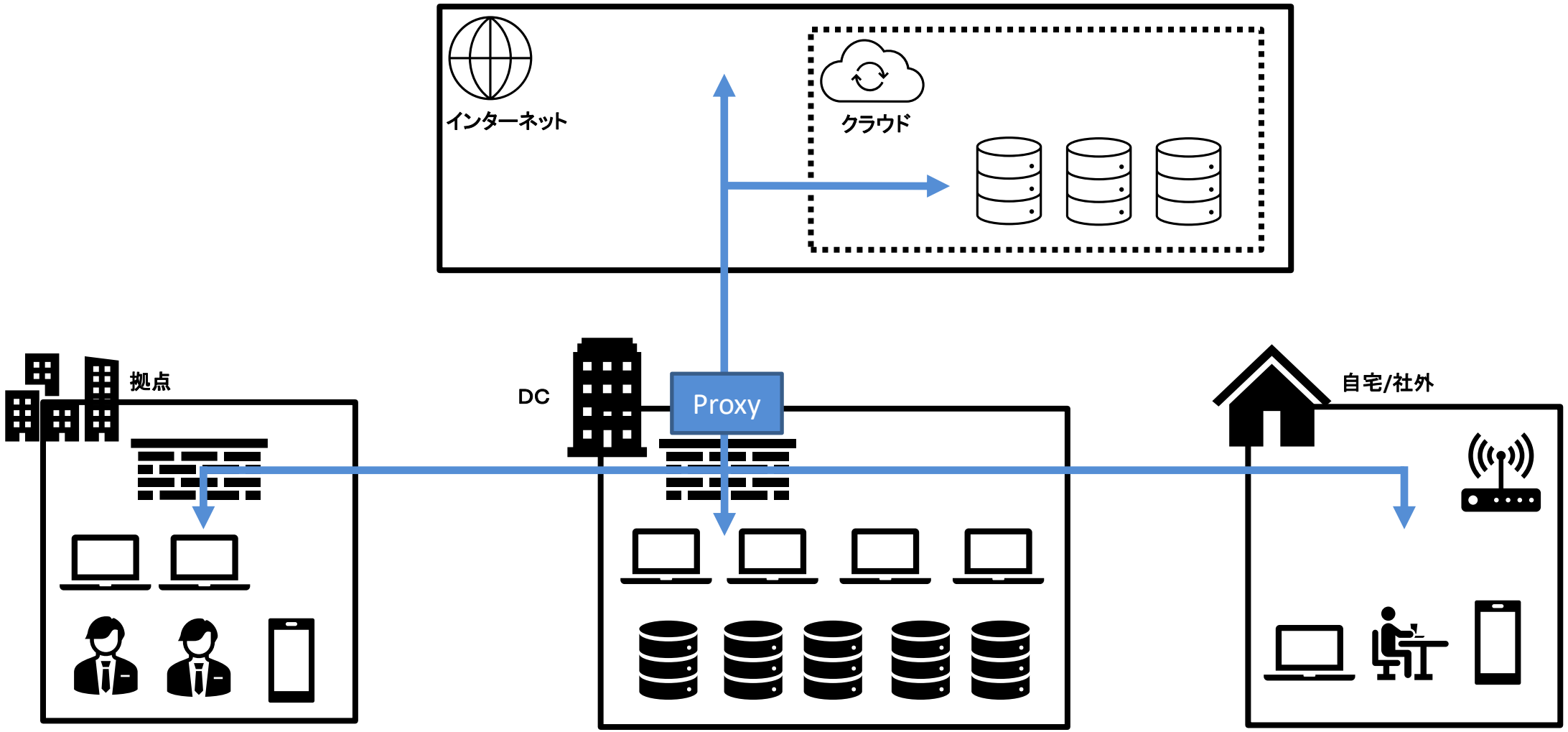
■モデルケースの想定環境としては、アンケート結果で最も多い下記の環境とする。

1. システムはオンプレとクラウド併用 

2. 業務拠点、データセンターがそれぞれ一つ 

3. 在宅環境(＋社外接続も可能)有り 

5. モデルケース概要(想定環境)



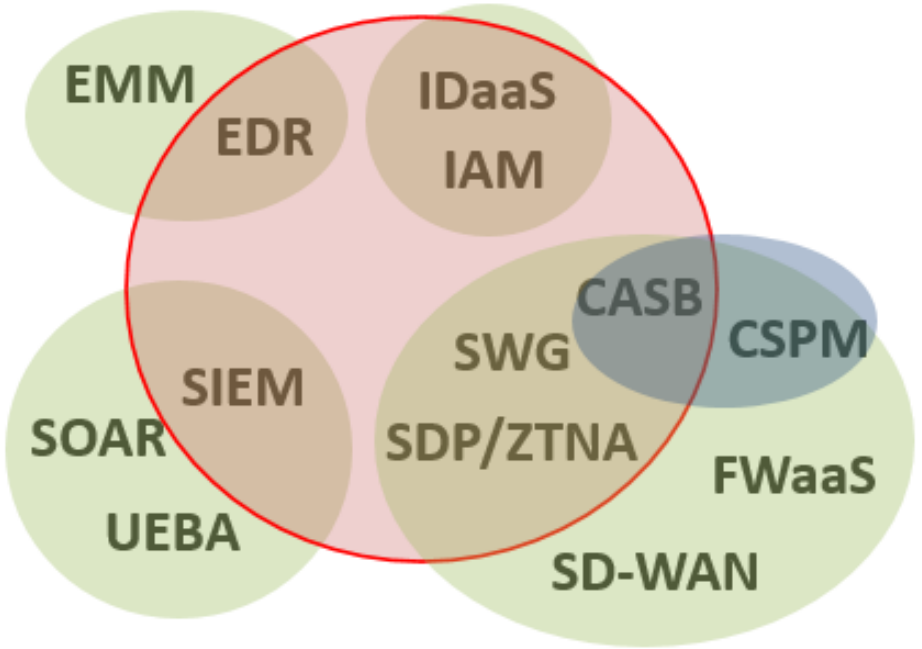
目次

6. モデルケース例

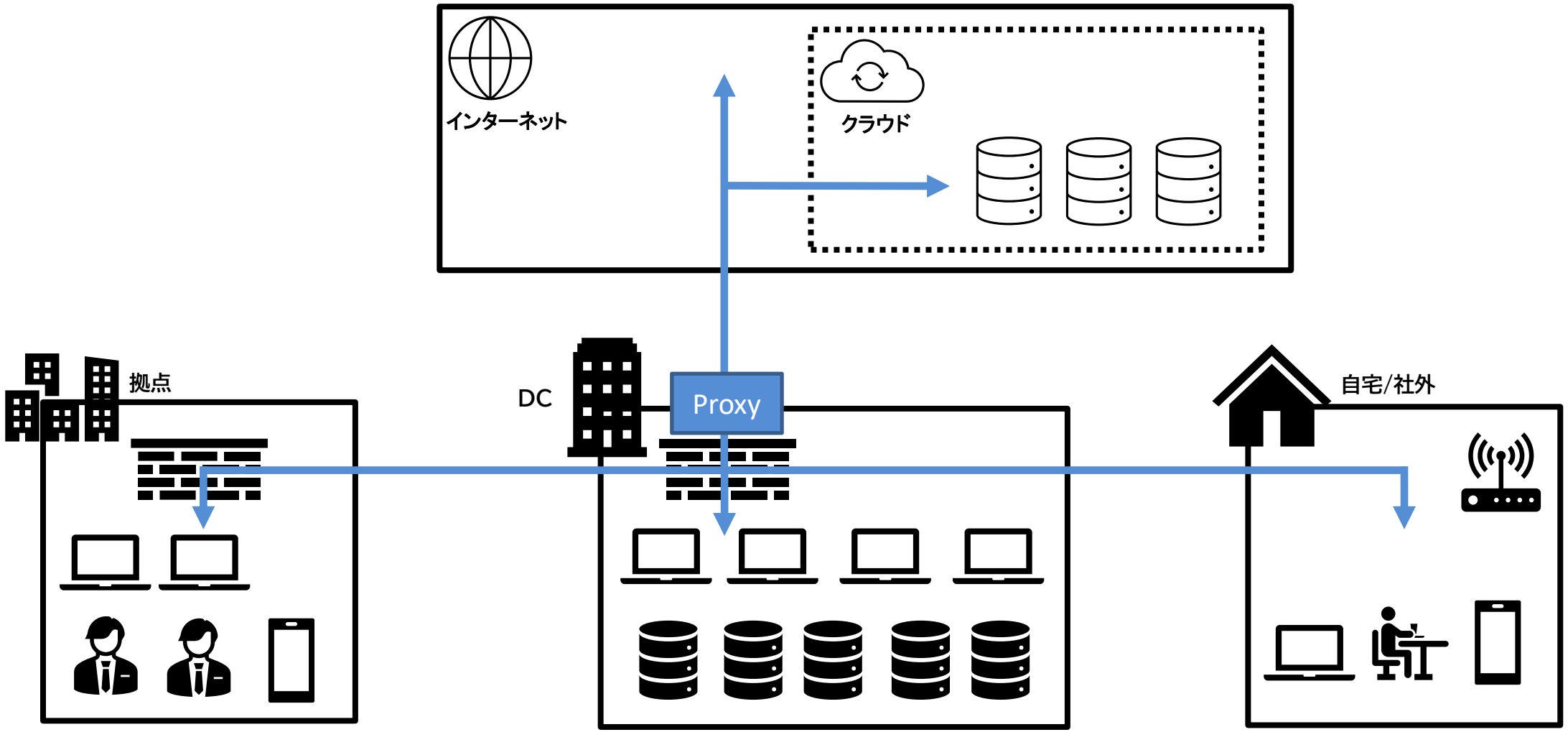
レベル1（最小限）

- 「マイクロセグメンテーション」、「MFA認証」、「ログ分析・監視」の3要素を導入
- SASEの内、セキュリティ機能を担う3要素(※)を導入

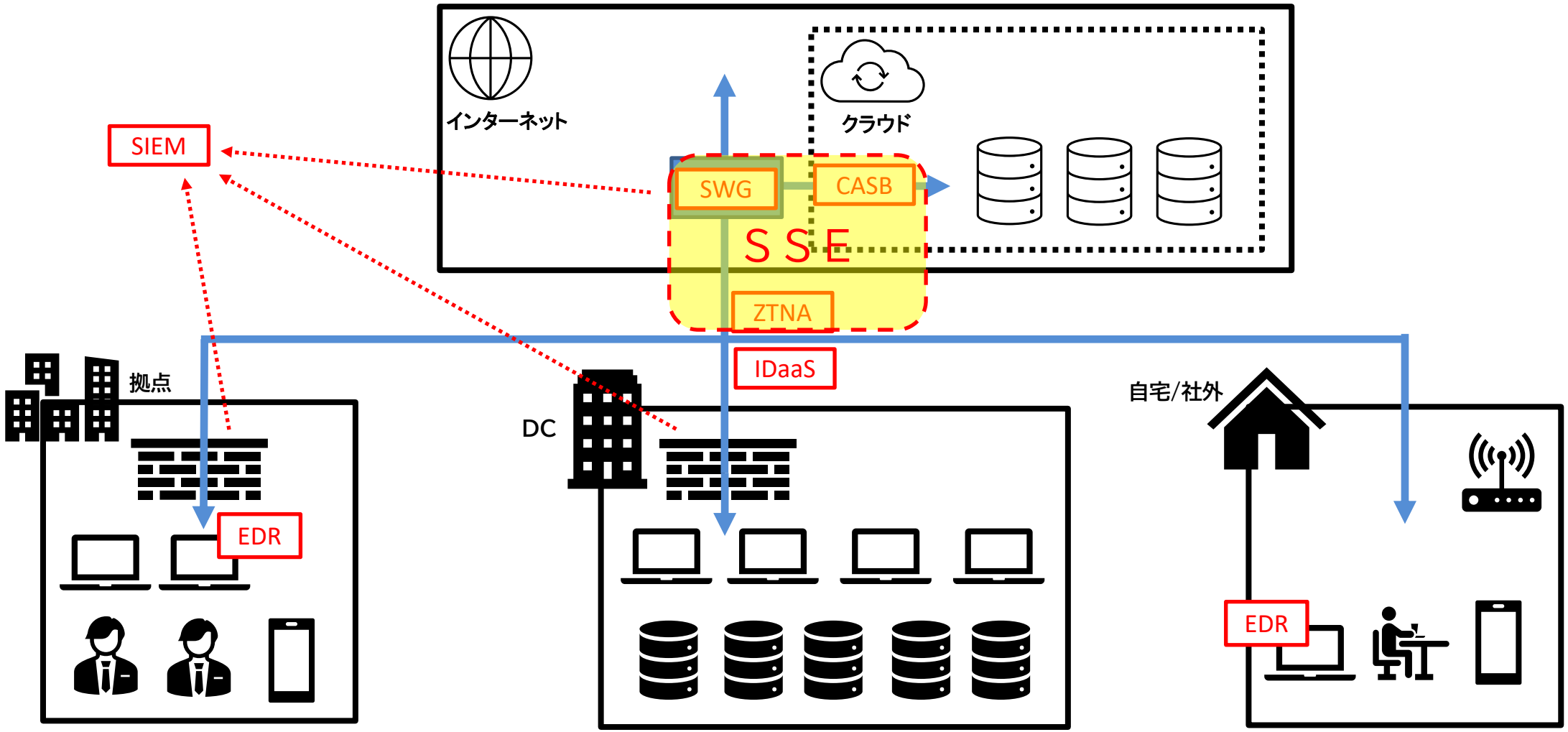
(※) SSE(Security Service Edge)：「CASB」、「SWG」、「ZTNA(SDP)」



6. モデルケース例



6. モデルケース例



6. モデルケース例(構成要素)

レベル1(最小限) の構成要素

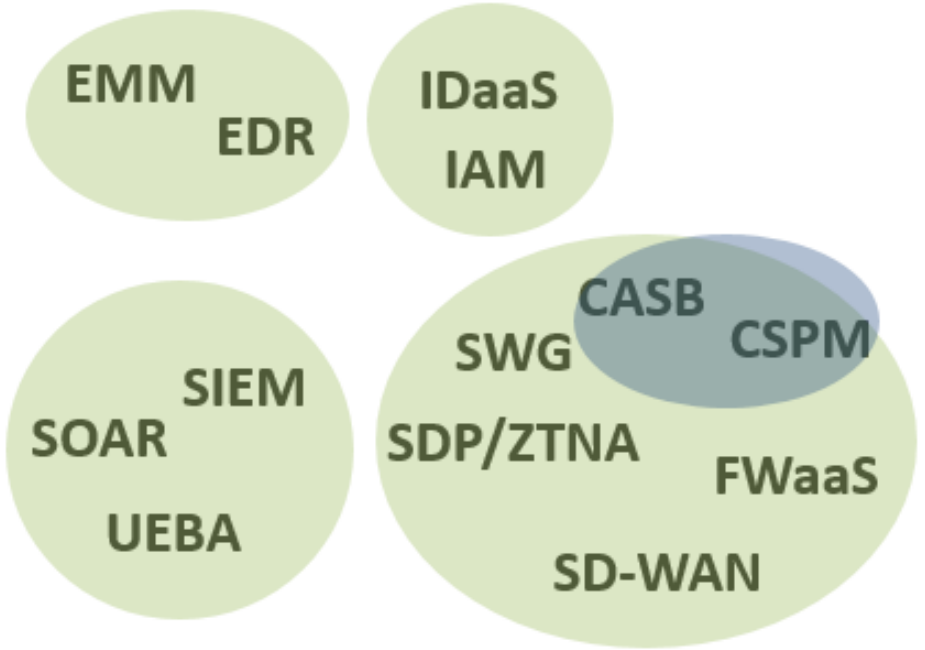
機能	ソリューション名	代表的な製品	概要
MFA認証	IDaaS	・Azure Active Directory ・Okta Identity Cloud	クラウド上の様々なサービスのID管理を一元的に行うソリューション。SaaS(Software as a Service)等への認証(多要素認証、シングルサインオン)・認可(アクセスコントロール)・ID管理・ID連携を行う機能を有する。
	IAM	・Azure Active Directory ・Okta Identity Cloud	ユーザーのIDとアクセス情報を管理し、本人確認(認証)、適切なアクセス権限の付与(認可)、SSO(シングルサインオン)等を行うソリューション。
ログ分析	SIEM	・Splunk ・Sumo Logic	様々な機器やソフトウェアのログを一元的に管理・蓄積し、セキュリティ上の脅威となる事象を検知・分析するためのソリューション。
マイクロセグメンテーション	CASB	・Cisco Umbrella ・Zscaler Internet Access	業務部門で契約しているものや個人で利用しているものも含め、自社で利用されているすべてのクラウドサービス(SaaS)の利用の可視化、安全性評価、通信遮断等の管理・制御を行うためのソリューション。
	SWG	・Cisco Umbrella ・Zscaler Internet Access ・i-FILTER	業務上不要なWebサイトへのアクセス制限やダウンロードしたファイルのチェック等のWebサイトへのアクセス制御機能をクラウド型で提供するソリューション。
	ZTNA (SDP)	・Cisco Secure Access by Duo ・Zscaler Private Access	オンプレミスやクラウド上のITシステム等に対するユーザーからネットワーク接続要求を、コントローラーが中心となり、IAMと連携して認証・認可するソリューション。アクセスが許可されると、ユーザー側とアクセス先のITシステム等の間で、直接仮想通信網が構築されるが、一連の通信が終了すると仮想通信網は消滅するなど、境界がソフトウェアにより動的に構成・制御される。
デバイスセキュリティ	EDR	・Symantec Endpoint Protection ・Cybereason EDR	デバイスやサーバにおけるサイバー攻撃を検知する。エンドポイント上の挙動に関わる情報を収集・分析し、不審な挙動を検知した場合は、迅速に対応(隔離や機能停止)を行うことで、ラテラルムーブメント等による被害や影響の拡大を防ぐことを支援するソリューション。

6. モデルケース例

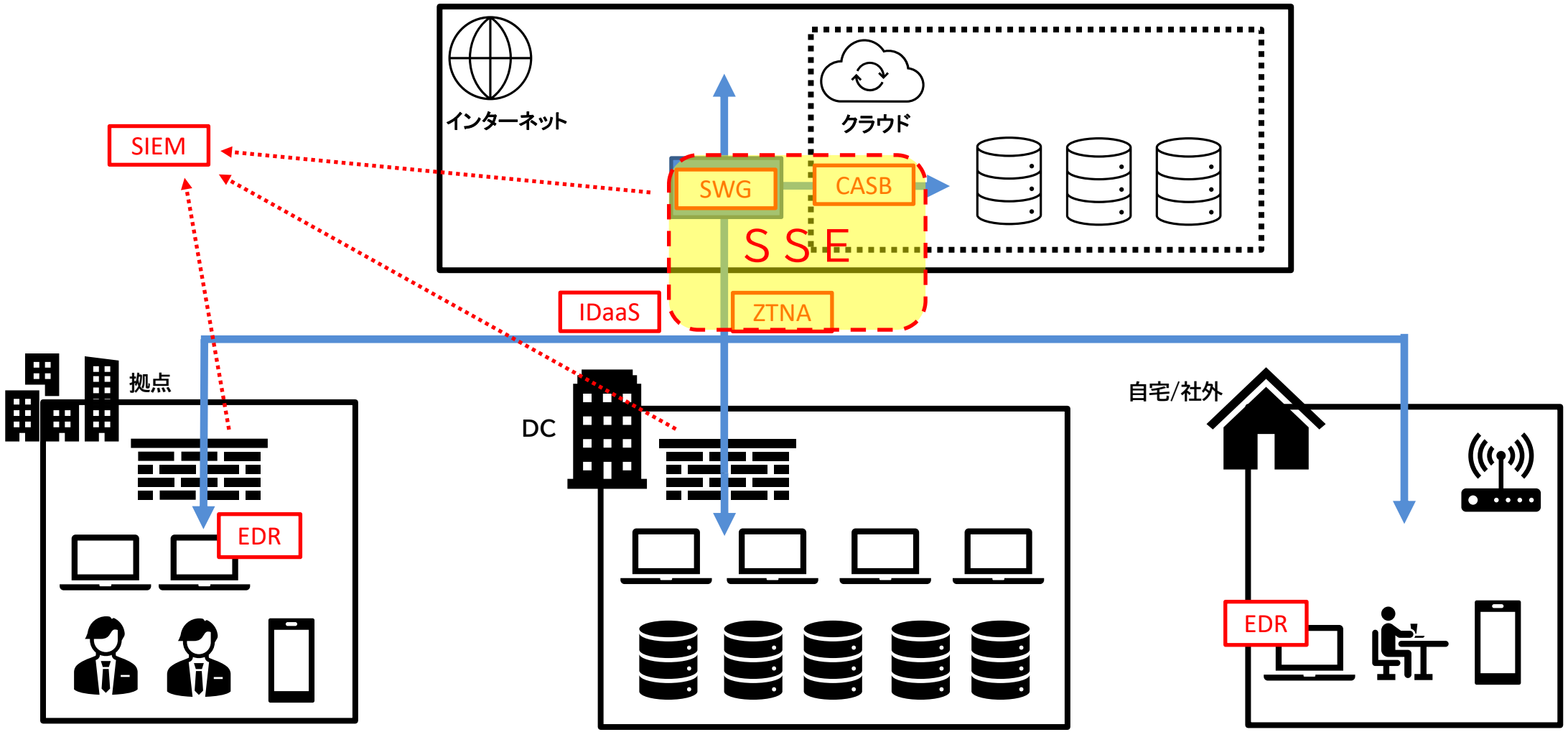
レベル2

- レベル1で導入した機能と連携、拡張させる要素（機能面、運用面での向上）
- SASEの内、レベル1で導入していない要素(※)

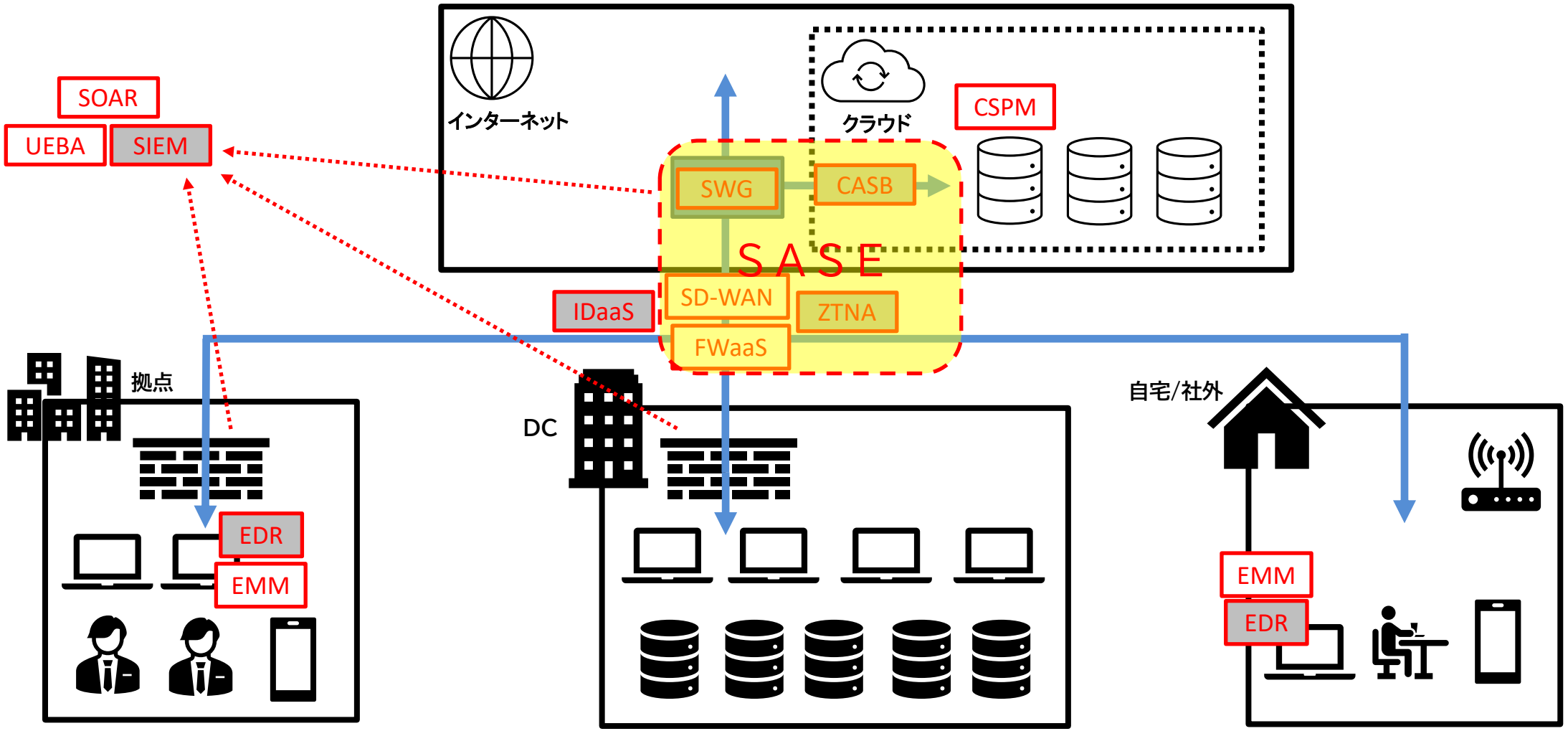
(※)「SD-WAN」、「FWaaS」



6. モデルケース例



6. モデルケース例



6. モデルケース例(構成要素)

レベル2の構成要素

機能	ソリューション名	代表的な製品	概要
ログ分析	SOAR	・FortiSOAR ・Splunk SOAR	脅威情報の管理・分析・優先度付け、インシデント管理の可視化・効率化、既知インシデントに対する定型対応の自動化等により、セキュリティ運用の自動化・効率化を実現するためのソリューション。
	UEBA	・Azure Sentinel ・Sumo Logic	機械学習等を利用してユーザーや機器の行動を分析し、通常と異なるユーザーの振る舞いを異常行動として検知するソリューション。
SASE (複数のソリューションを含む製品が多い)	CSPM	・prisma cloud ・Cloudbase	IaaS PaaS に対して セキュアな設定がなされていることを継続的に評価し 適切な設定への修正を支援するソリューション 。 クラウド側の設定を自動的に確認し、設定ミスや各種ガイドライン等への違反が無いかを継続してチェックすることができるものもある。
	SD-WAN	・Cisco SD-WAN ・Prisma SD-WAN	ネットワークをソフトウェアで制御するSDN(Software Defined Networking)を物理的なネットワーク機器で構築したWANに適用するソリューション。企業の拠点間接続やクラウド接続などにおいて柔軟なネットワーク構成、トラフィックコントロールなどを実現する。
	FWaaS	・prisma Access ・Zscaler cloud firewall	ファイアウオール機能をそのままAs a Serviceとしてクラウドで提供するソリューション。 利用者はクラウド上のファイアウォールを介して外部と通信するため、ネットワーク管理者にとっても、複数拠点のファイアウォールを管理する必要がなく、単一のFWaaSのみを管理する。運用自体はクラウドサービス事業者が行うため、機材の交換やソフトウェアの更新などのメンテナンス業務も軽減される。
デバイスセキュリティ	EMM	・CLOMO ・LanScope Cat	スマートフォンやタブレット等 のモバイル端末を総合的に管理するソリューション。ネットワークやセキュリティのポリシーに従った設定を行い、機能の有効化や不要な機能の制限等を行える。

目次

7. まとめ

■分科会2の研究成果

ゼロトラストってなんだろう？

- ゼロトラストの概念を説明
- 最小限の構成要素を調査

導入イメージが分からない

- アンケートを実施して実態調査
- モデルケースを提示

これからゼロトラストを導入する際に参考としてください。

最後に・・・

今回のJUAS研究会を終えて・・・

- 曖昧だったゼロトラストの概念や構成要素について知見を深めることができた。
- アンケートを通して他企業の導入状況や構成について知ることができた。
- 他企業の動向やセキュリティの思想を知ることができた。
- アンケートによる実態調査をもとに、ゼロトラスト導入のモデルケースを提案することができた。
- ゼロトラストについて自分なりの解釈ができ、導入に際し提言することができた。
- 多くの企業の方々と話をする機会が得られ、モチベーションが向上した。

2023年度 ITインフラ研究会
分科会3

理想の共通インフラ基盤の構成とは

クラウド化が進む中で現状の構成はどうあるべきか

2023年4月

分科会3

アジェンダ

1. 研究テーマ、テーマ選択の背景、ゴール
2. インフラ構成の分類
3. 要件の整理
4. 各インフラ構成の特徴
5. 仮説
6. アンケートについて
7-1. アンケート結果(サマリ)①
7-2. アンケート結果(サマリ)②
7-3. アンケート結果(サマリ)③
8-1. アンケート分析①
8-2. アンケート分析②
9-1. 理想の構成について①
9-2. 理想の構成について②

1. 研究テーマ、テーマ選択の背景、ゴール

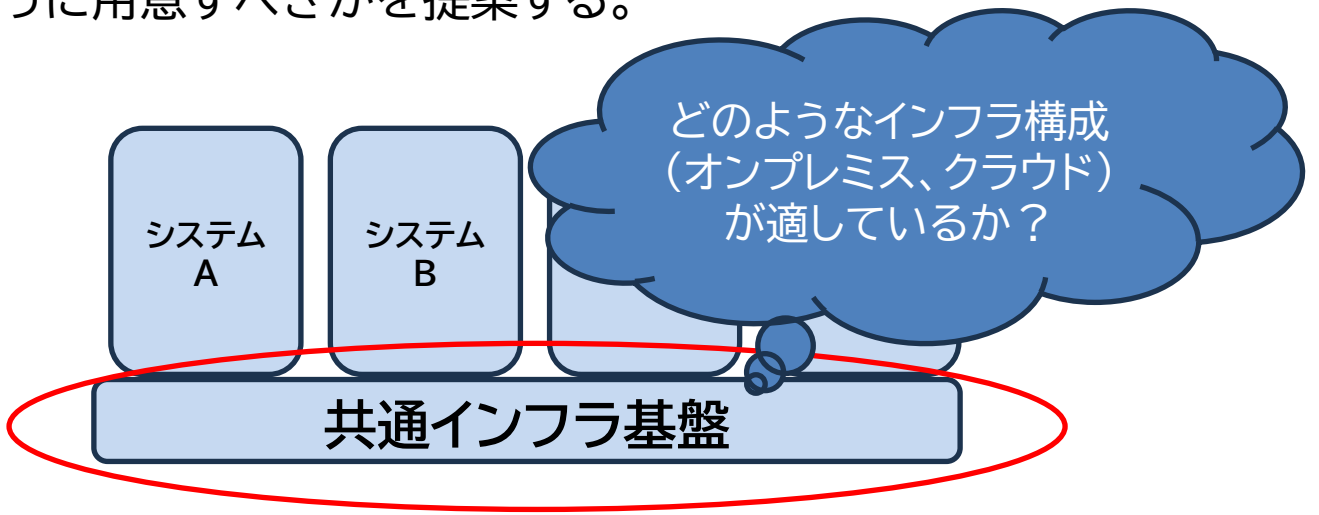
- **研究テーマ**
  - インフラ構成の選定基準には何があるか。

- **テーマ選択の背景**
  - 近年クラウド化が叫ばれ、各社で大なり小なりクラウドを利用し始めている。
  - 各社のインフラ構成について、クラウド化が進む一方でオンプレ回帰の動きもあり、インフラ構成が多様化している。
  - 個別システム向けのインフラ構成を選定する基準はよく議論されているが、
    複数システム向けの共通インフラ基盤を選定する基準についてはあまり議論されていない。

- **ゴール**
  - 全体最適となるような共通インフラ基盤をどのように用意すべきかを提案する。

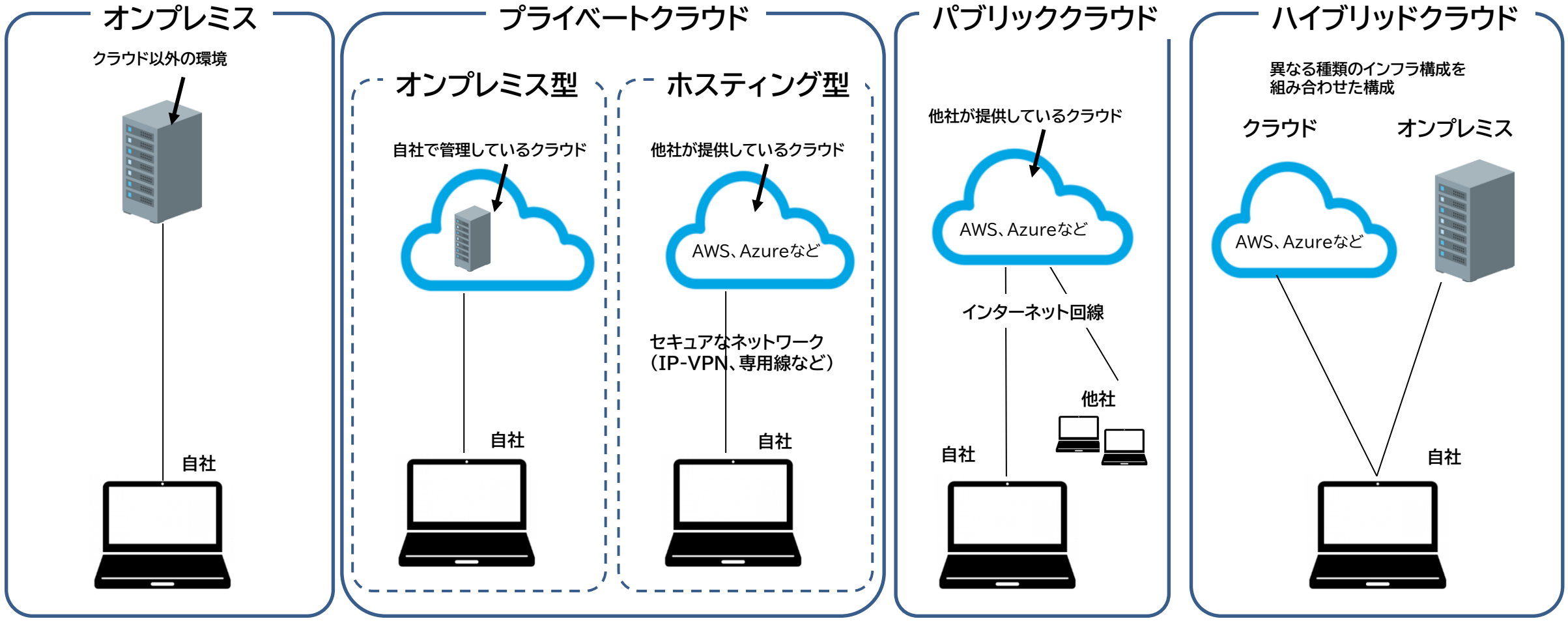
※共通インフラ基盤

個々のアプリケーションの制約を考慮した個別システムのインフラではなく、
中小規模の社内システムの集合体が稼働する標準インフラ(右図)と
定義した。



2. インフラ構成の分類

■ 理想の共通インフラ基盤を考えるにあたり、分科会3では以下5種類のインフラ構成があると定義した。



3. 要件の整理

■分科会3内で共通インフラ基盤の現状と理想を確認したが、各社や業界によりインフラ構成や方針が異なる。
■それぞれのインフラ基盤を選定するにあたり、各社で重視する要件があった。

分科会3各社で採用しているインフラ構成	
メーカー企業	公共インフラ企業
パブリッククラウド プライベートクラウド ハイブリッドクラウド	パブリッククラウド ハイブリッドクラウド

業界の観点だけでは
インフラ構成の傾向は
わからなかった

要件(非機能要件＋コスト)により、
インフラ構成に傾向がある？

■プライベートクラウド
性能・拡張性

■パブリッククラウド
移行性、コスト

■オンプレミス
セキュリティ

■ハイブリッドクラウド
可用性

4. 各インフラ構成の特徴(1/2)

■参考文献(※)をもとに、各インフラ構成について、非機能要件＋コストの観点で特徴を整理した。
各特徴を優れている順に◎(青字)、〇、△(赤字)で記載した。

観点＼種類	オンプレミス	プライベートクラウド（オンプレミス型）	プライベートクラウド（ホステッド型）	パブリッククラウド	ハイブリッドクラウド
可用性	◎リソース、ネットワークの品質・配置を最適化し、可用性を向上できる。	◎リソース、ネットワークの品質・配置を最適化し、可用性を向上できる。	〇リソース、ネットワークの品質・配置をある程度最適化し、可用性を向上させやすい。	△リソース、ネットワークの品質・配置を最適化しずらく、可用性を向上させにくい。	◎リソース、ネットワークの品質・配置を最適化し、可用性を向上できる。
性能・拡張性	◎リソース、ネットワークの品質・配置を最適化し、性　能を向上できる。 △ハードウェア調達などが必要なため、迅速にリソースを増強できない。	◎リソース、ネットワークの品質・配置を最適化し、性能を向上できる。 〇ハードウェア調達などが不要であれば、迅速にリソースを増強できる。	〇リソース、ネットワークの品質・配置をある程度最適化し、性能を向上させやすい。 ◎ハードウェア調達が不要なため、迅速にリソース増強できる。	△リソース、ネットワークの品質・配置を最適化しずらく、性能を向上させにくい。 ◎ハードウェア調達が不要なため、迅速にリソース増強できる。	◎リソース、ネットワークの品質・配置を最適化し、性能を向上できる。 〇ハードウェア調達などが不要であれば、迅速にリソース増強できる。
運用・保守性	◎リソース、ネットワークを管理できるため、障害個所の特定・ライフサイクルをコントロールしやすい。 〇オンプレミスのスキルを持つ要員が必要である。	◎リソース、ネットワークを管理できるため、障害個所の特定・ライフサイクルをコントロールしやすい。 △オンプレミスとクラウドの両スキルを持つ要員が必要である。	〇リソース、ネットワークの配置範囲をある程度管理できる可能性があり、障害箇所を特定しやすい。 〇クラウドのスキルを持つ要員が必要である。	△リソース、ネットワークの配置範囲が広く、障害箇所の特定が難しい。 〇クラウドのスキルを持つ要員が必要である。	△構成が複雑になり、運用・保守しづらくなる可能性がある。 △各環境のスキルを持つ要員が必要である。
移行性	◎移行要件を満たすために作りこみが可能である。 △移行先の構築に時間がかかる。	◎移行要件を満たすために作りこみが可能である。 △移行先の構築に時間がかかる。	〇クラウドの制約により、移行要件を満たせない可能性がある。 ◎移行先を迅速に構築できる。	〇クラウドの制約により、移行要件を満たせない可能性がある。 ◎移行先を迅速に構築できる。	◎移行要件を満たすために作りこみが可能である。 △移行先の構築に時間がかかる。

※セキュリティ関連NIST文書について.「クラウドコンピューティングの概要と推奨事項」.https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000025367.pdf、(2024/03/04)

4. 各インフラ構成の特徴(2/2)

■参考文献(※)をもとに、各インフラ構成について、非機能要件＋コストの観点で特徴を整理した。
各特徴を優れている順に◎(青字)、〇、△(赤字)で記載した。

観点＼種類	オンプレミス	プライベートクラウド(オンプレミス型)	プライベートクラウド(ホステッド型)	パブリッククラウド	ハイブリッドクラウド
セキュリティ	◎リソース、データを自組織に閉じた環境に配置し、コントロールできるため、セキュリティは高い。 ◎セキュリティの対応状況を実際に確認できる。	◎リソース、データを自組織に閉じた環境に配置し、コントロールできるため、セキュリティは高い。 ◎セキュリティの対応状況を実際に確認できる。	〇クラウド提供元がリソースを管理するが、自組織が占有するため、外部から攻撃される可能性は高くない。 △クラウド提供者のセキュリティ対策状況を実際に確認できない。	△インターネット経由でリソースに接続するため、外部から攻撃される可能性が高くなる。 △クラウド提供者のセキュリティ対策状況を実際に確認できない。	◎重要なリソース、データをオンプレミス・プライベートクラウド(オンプレミス型)内に配置することでセキュリティを担保できる。 〇オンプレミス・プライベートクラウド(オンプレミス型)に関しては、セキュリティの対応状況を確認できる
システム環境・エコロジー	◎システムの設置環境を把握・コントロールしやすい。	◎システムの設置環境を把握・コントロールしやすい。	〇システムの設置環境をある程度把握・コントロールできる可能性がある。	△システムの設置環境を基本的に把握・コントロールできない。	〇オンプレミス・プライベートクラウド(オンプレミス型)に関しては、設置環境を把握・コントロールしやすい。
コスト	〇ソフトウェア、ハードウェア、設備が必要なため、初期費用は高い。 △従量課金でないため、初期費用は高い。	△クラウド実装に必要なソフトウェア、ハードウェア、設備が必要なため、初期費用は非常に高い。 △従量課金でないため、初期費用は高い。	〇クラウド実装に必要なソフトウェア、ハードウェア、設備は不要だがネットワークは安価でないため、初期費用は高い。 ◎従量課金であるため、初期費用は安い。	◎クラウド実装に必要なソフトウェア、ハードウェア、設備が不要であり、ネットワークも安価なため、初期費用は安い。 ◎従量課金であるため、初期費用は安い。	△複数環境を利用するため、各環境の利用、連携に必要な初期費用が高い。 〇オンプレミス・プライベートクラウド(オンプレミス型)以外は従量課金のため、初期費用は安い。

※セキュリティ関連NIST文書について.「クラウドコンピューティングの概要と推奨事項」.https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000025367.pdf、(2024/03/04)

5. 仮説

■理想とするインフラ構成は、重視する要件（非機能要件+コスト）により決まると仮定した。
各インフラ構成の特徴をもとに、重視する要件を算出（◎を3点、〇を2点、△を1点とした平均点の上位3つ）した。

インフラ構成の種類	重視する要件（◎を3点、〇を2点、△を1点とした平均点）
オンプレミス	可用性（3）、セキュリティ（3）、システム環境・エコロジー（3）
オンプレミス型プライベートクラウド	可用性（3）、セキュリティ（3）、システム環境・エコロジー（3）
ホステッド型プライベートクラウド	性能・拡張性（2.5）、移行性（2.5）、コスト（2.5）
パブリッククラウド	コスト（3）、移行性（2.5）、性能・拡張性（2）
ハイブリッドクラウド	可用性（3）、性能・拡張性（2.5）、セキュリティ（2.5）

6. アンケートについて

■ITインフラ研究会内でアンケートを実施

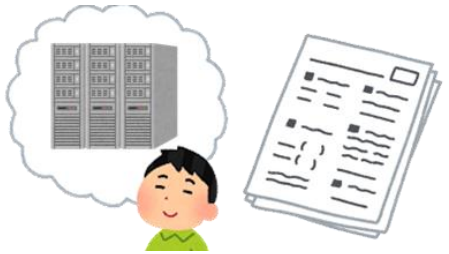
アンケート対象者：2023年度 JUAS ITインフラ研究会 参加メンバー

アンケート期間：2023/12/14～2023/12/31

回答者数：21名

アンケートの目的：

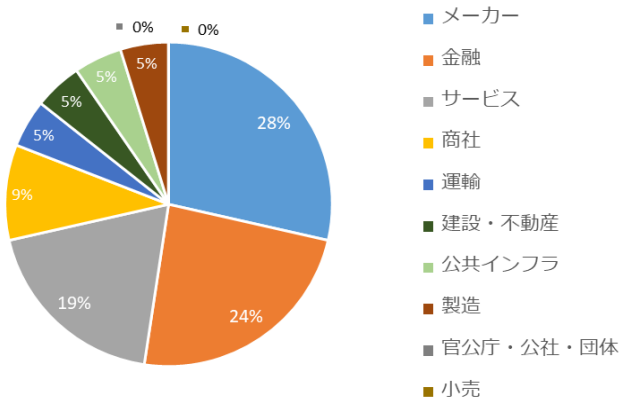
- 各社の現状と理想の共通インフラ構成について把握する。
- 分科会3の仮説とアンケート結果を比較分析し、整合性やギャップを明らかにする。
- 分析結果から全社で利用する際の理想的なインフラ構成を提示する。



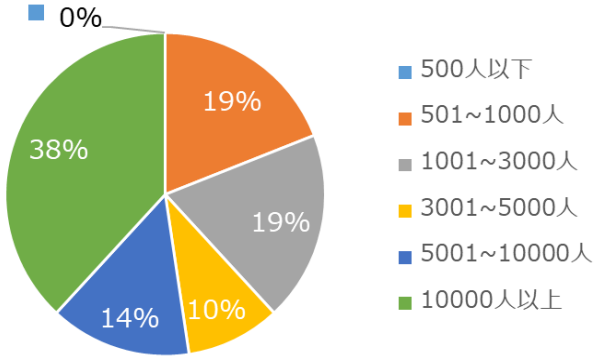
7-1. アンケート結果(サマリ)①

■8つの業種および会社規模が異なる担当者より、アンケート回答をいただいた。
■共通インフラ基盤の利用レベルとしては、IaaSが最も多く、一部SaaSとしての利用があった。

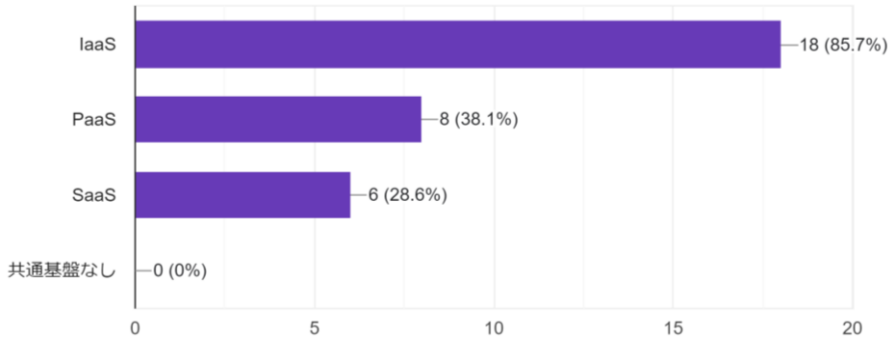
業種を教えてください
21件回答



従業員数を教えてください
21件回答

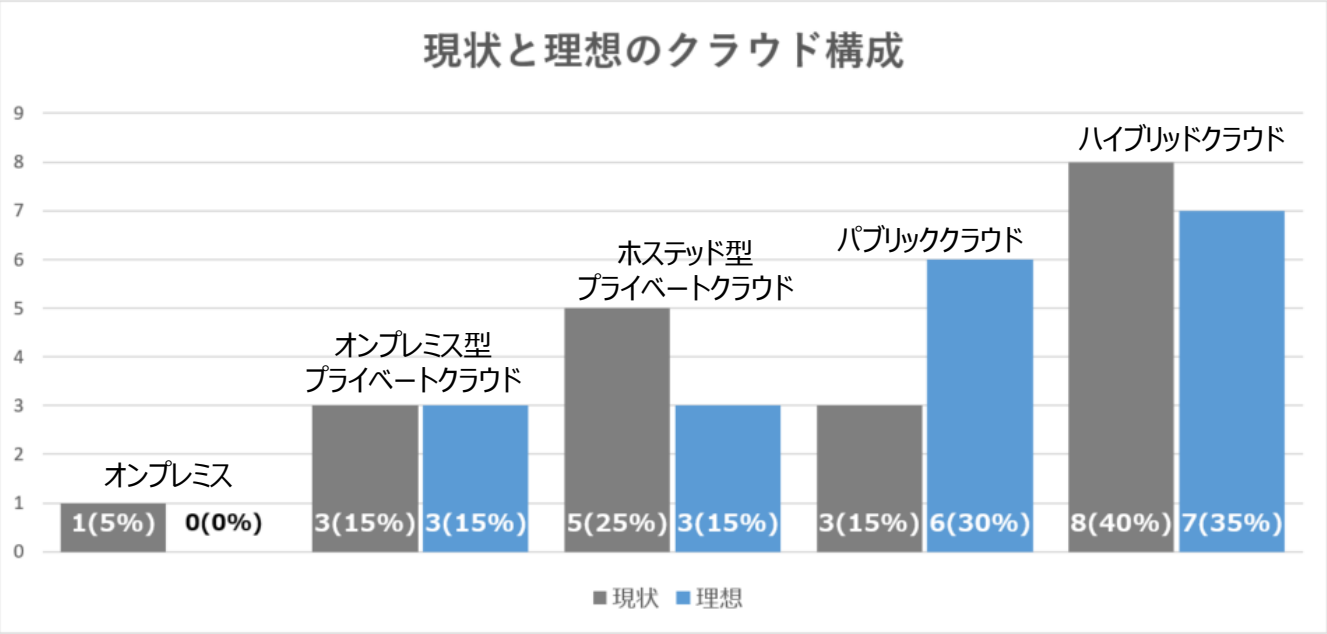


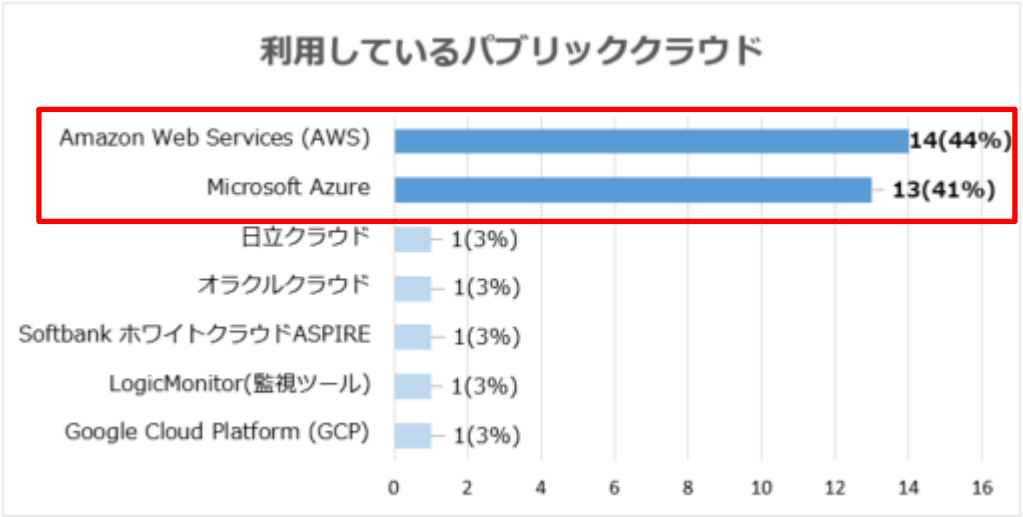
共通インフラ基盤の利用レベルを教えてください
21件回答



7-2. アンケート結果(サマリ)②

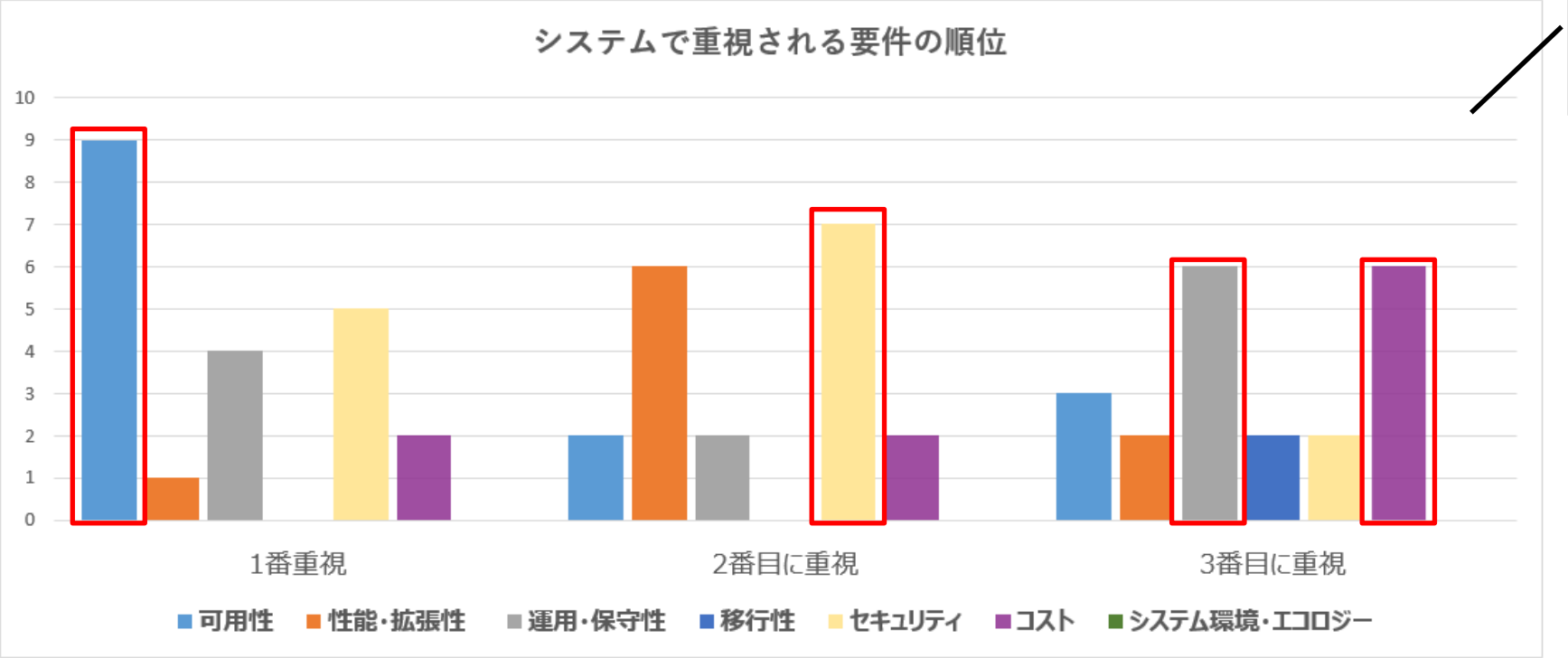
■現状のインフラ構成として全体の95%がクラウドを利用しており、全体の40%がハイブリットクラウドであった。
■オンプレミスを理想としている企業はなく、ハイブリットクラウド(35%)やパブリッククラウド(30%)の割合が高い。
■クラウドベンダでは、AWSとAzureを利用している企業が多い傾向がある。





7-3. アンケート結果(サマリ)③

■システムで重視される要件は、可用性、セキュリティ、運用・保守性、コストであった。
■複数のアプリケーションが稼働する基盤であるため、安心安全に稼働するインフラ基盤が求められている。
■一方で、システム環境・エコロジーは重要度が低くなっており、重視している企業はなかった。



1番重視:**可用性**
2番重視:**セキュリティ**
3番重視:**運用・保守性、コスト**

回答理由

・業務の安定的な遂行が会社の使命だから

・要件として、可用性とセキュリティを重要視するアプリが多いため

・共通基盤としてセキュリティと運用が回ることが前提と考えるため

8-1. アンケート分析①

■アンケート結果から重視される要素(非機能要件＋コスト)は仮説と異なっており、
可用性、運用・保守性、コスト、セキュリティであった。
■アンケート結果から重視される要素に含まれる課題(赤字)は約半数(46%)であった。
※ オンプレミスを理想のインフラ構成とするアンケート結果はなかったため、以下の表からオンプレミスを除外している。

凡例
↑:仮説よりも重視されていた
↓:仮説よりも軽視されていた
→:想定通りの重要度
＋:想定外の重視項目

種類	仮説から重視される要素	アンケート結果から重視される要素		この構成にするために抱えている課題
オンプレミス型プライベートクラウド	可用性、セキュリティ、システム環境・エコロジー	可用性(24%)	→	可用性(21%)
	ー	運用・保守性 (21%)	＋	運用・保守性(18%)、移行性(18%)、セキュリティ(18%)
	ー	コスト(15%)	＋	ー
ホステッド型プライベートクラウド	性能・拡張性、移行性、コスト	セキュリティ(23%)	＋	性能・拡張性(46%)
	ー	性能・拡張性(18%)	↓	コスト(38%)
	ー	運用・保守性(17%)	＋	運用・保守性(17%)
パブリッククラウド	コスト	セキュリティ(19%)	＋	運用・保守性(39%)
	移行性	コスト(19%)	↓	性能・拡張性(29%)、コスト(29%)
	性能・拡張性	可用性(18%)	＋	ー
ハイブリッドクラウド	可用性	可用性(22%)	→	セキュリティ(25%)
	性能・拡張性、セキュリティ	コスト(19%)	＋	性能・拡張性(21%)、運用・保守性(21%)
	ー	運用・保守性(17%)	＋	ー

8-2. アンケート分析②(1/2)

■理想のインフラ構成にする上で、アンケート結果から重視される要素と同じ課題が重要と考え、
”想定される問題”と”解決策の提案”を記載した。

※ オンプレミスを理想のインフラ構成とするアンケート結果はなかったため、以下の表からオンプレミスを除外している。

種類	課題	想定される問題	解決策の提案
オンプレミス型 プライベートクラウド	可用性	1）DRサイトの構築にかかる導入コストが高く、大規模な災害が発生した時の可用性を担保しにくい。 2）障害発生時に他社ではなく、自社で対応する必要があり、他社よりも復旧作業に時間がかかる。	1）最低限の運用に必要な構成に留めることで、導入コストを抑制しつつ、DRサイトを構築し可用性を高める。 2）運用・保守体制を整備する。必要に応じて保守サービスの契約レベルを上げる。
	運用・保守性	1）オンプレミス環境の運用・保守には専門的な知識とリソースが必要であり、日々の管理作業が負担になることがある。 2）自社でクラウド環境を運用する必要がある。大量のハードウェアの運用(リソース増強・障害対応など)が大変である 3）自社でソフトウェアなどのバージョン管理、資産管理する必要がある。	1）運用・保守体制を整備する。必要に応じて保守サービスの契約レベルを上げる。極力、仮想化基盤を同一の構成として、運用・保守しやすくする。 2）同上 3）ソフトウェアとハードウェアの資産管理・ライフサイクル管理を自動化するツールを導入し、運用負荷を軽減する。
ホステッド型 プライベートクラウド	性能・拡張性	1）拡張性は担保できるが、性能を確保できない可能性がある。	1）自社とホステッド型プライベートクラウド間を、品質の高いネットワークで 接続する。
	運用・保守性	1）予告なくGUI画面が変更になり、運用手順書の更新が大変である。 2）サービス提供期間がクラウドベンダーにコントロールされ、自社でライフサイクルをコントロール出来ない。 3）クラウド内の通信影響を伴うメンテナンス時間をコントロールできる期間が決まっている。	1）比較的変化が少ない手順(CLIなど)で運用手順書を作る。 2）極力、多くの利用者が使っている機能を使う。利用者が少なく、廃止される可能性が高い機能は使わない。ライフサイクルをコントロールしたい機能については、自社で構築する。 3）クラウド提供元のメンテナンス通知をキャッチアップする体制を作り、余裕をもってメンテナンス期間をコントロールする

8-2. アンケート分析②(2/2)

■理想のインフラ構成にする上で、アンケート結果から重視される要素と同じ課題が重要と考え、
”想定される問題”と”解決策の提案”を記載した。

※ オンプレミスを理想のインフラ構成とするアンケート結果はなかったため、以下の表からオンプレミスを除外している。

種類	課題	想定される問題	解決策の提案
パブリック クラウド	コスト	1）リソースの過剰利用や不適切なリソース管理により、ランニングコストが予想以上に増加する可能性がある。	1）課金の仕組みを把握し、課金が高くならないように構成を設計する。 ※例)特定区間の通信量に従量課金される場合、特定区間で大量の通信（バックアップ通信など)をしないなど。 クラウド提供元が公開しているコスト管理ツールにより、コストが増加している原因を調査/対応する。
ハイブリッド クラウド	セキュリティ	1）異なる環境間におけるセキュリティポリシーの一貫性の欠如により、セキュリティリスクが発生する可能性がある。 2）パブリッククラウドと他環境を組み合わせる時に、セキュリティリスクが高まる。 3）オンプレミス、オンプレミス型プライベートクラウド以外におけないデータがある。	1）システム全体でセキュリティポリシーを統一し、ポリシーに従いデータ配置、通信経路、運用手順などを決定する。 2）パブリッククラウドではなく、ホステッド型プライベートクラウドを採用し、他環境と組み合わせる。 3）重要なデータは安全な場所(オンプレミス、オンプレミス型プライベートクラウド)に退避する。
	運用・保守性	1）異なる環境の混在により、運用・保守が複雑化し、管理が困難になる。 2）環境毎のスキルを持った要員が必要になる。	1）ハイブリッドクラウドをサポートする管理プラットフォームを使用して、異なる環境を一元管理する。システム全体として、極力少ない設定変更で運用可能にする。 2）教育により要員のスキルを強化したり、外注して要員を準備する。

9-1. 理想の構成について①（非機能要件）

■仮説およびアンケート結果から重視される非機能要件によって、理想の共通インフラ基盤の構成は異なる。
■非機能要件のメリット・デメリットを参考にしながら、共通インフラ基盤の構成を選定していく必要がある。

重視する非機能要件	理想の共通インフラ基盤のモデル
可用性	オンプレミス型プライベートクラウド、パブリッククラウド、ハイブリッドクラウド
性能・拡張性	ホステッド型プライベートクラウド
運用・保守性	オンプレミス型プライベートクラウド、ホステッド型プライベートクラウド、ハイブリッドクラウド
移行性	該当なし ※アンケート結果から重視される要素には含まれていなかった。
セキュリティ	ホステッド型プライベートクラウド、パブリッククラウド
システム環境・エコロジー	該当なし ※アンケート結果から重視される要素には含まれていなかった。
コスト	オンプレミス型プライベートクラウド、パブリッククラウド、ハイブリッドクラウド

9-2. 理想の構成について②(インフラ構成)

■仮説およびアンケート結果から各インフラ構成によって重視される非機能要件は異なる。
■非機能要件のメリット・デメリットを参考にしながら、共通インフラ基盤の構成を選定していく必要がある。

実装したい共通インフラ基盤のモデル	重視される非機能要件
オンプレミス型プライベートクラウド	可用性、運用・保守性、コスト
ホステッド型プライベートクラウド	セキュリティ、性能・拡張性、運用・保守性
パブリッククラウド	セキュリティ、コスト、可用性
ハイブリッドクラウド	可用性、コスト、運用・保守性

まとめ

- 各社の要件に応じて、最適と思われる共通インフラ基盤の構成を提案できた。
  加えて、課題になり得る問題と解決策も提案できた。
- 今回、アンケートの回答数は21件と多くなかったが、回答内容を定量化し、関係性を分析することで
  傾向を把握できた。
- 普段は知り得ない他社のシステムに対する考え方などを知ることができ有意義な研究となった。

2023年度 ITインフラ研究会
分科会4

インフラ開発案件リリースに向けた品質向上施策における研究

レビューで安心・安全なITインフラを創る

2024年4月

分科会4

1. 緒言

■ 緒言

- ITシステムは私たちにとって身近で、生活に欠かせないものになっており、ユーザー企業のIT部隊で働く私たちが取り扱うシステムも、生活に欠かせなく、サービス停止が発生しないように、ITサービスの品質向上を努めている。
- ITインフラ部隊はシステムの基盤となる部分を担っており、障害が発生したときのインパクトが大きいため、日々障害が発生しないように、各社で向上施策を検討・実施し、独自ナレッジを有していると考える。
- 各社ナレッジを可能な限り共有・比較検討し、ITインフラ部隊の更なる品質向上を目指したい。

2. 背景/目的

■ テーマを選定した背景
- 昨今ではシステムの障害発生が大きな社会問題になっている。
- 障害を未然に防ぎ、システムを安定稼働させることが最重要課題であると考えるため、本研究によって更なる品質向上を目指す。

■ 目的
- システム障害を未然に防ぎ、安定稼働をさせるために、各社の品質向上ナレッジを集約し、更なる品質向上を目指す。

3. 研究方針

■ 研究の進め方
- 各社の品質向上施策のヒアリング実施
  - ウォーターフォールモデルをもとに各工程でどのような品質向上施策を実施しているのか、ヒアリングを行う。
    ※ ヒアリングシートイメージは次スライドで説明を行う
- 品質向上策を比較、分類
  - 各社がヒアリングした結果を共有し、分類分けを行う。

3. 研究方針

- ヒアリングシートイメージ

各工程でどのようなタスクがあるかを記入

各タスクでどのような品質向上施策を行っているかを記入

	会議体	レビュー対象	趣旨	会議参加者（★はレビューアー）	会議時間(分)/工数（人日）	品質向上施策（会社として/個人として気を付けていること）
⑥	基盤変更管理会議	付議資料	基盤で発生する作業の対応方針の妥当性を確認する。	★部長、担当部長、グループリーダー、メンバー	30分から60分	基盤で発生する作業すべての対応方針の妥当性を確認する。 付議資料には目的、背景、対応概要、手順、コンチプラン、スケジュール、作業リスク、リスクへの対策などが記載されている。
⑦	運用調整会議	本業務運用作業一覧	本番環境での作業すべてを確認し協議、承認を行う。(リリース判定)	★本部長、部長	60分	本番環境で実施する作業について確認し、協議、承認を行う。

4. 品質向上施策のヒアリング結果分析

- A社(抜粋)

項目	矢羽
	要件発生 → 要件定義 → 基本設計 → 各種設計 → 開発/テスト → リリース → 運用開始
要件定義	①ユーザ要望ヒアリング ②ベンダーへの見積打合せ（要件定義） ③受注伺い書の作成、レビュー ④見積もり説明打合せ
基本設計	
各種設計	⑤設計書(設計、切替、ﾃｽﾄ)ﾚﾋﾞｭｰ ⑥ベンダードｷｭﾒﾝﾄﾚﾋﾞｭｰ ⑦ユーザとの切替調整
開発/テスト	⑧構築結果確認 ⑨完了報告
リリース	⑪成果物ﾚﾋﾞｭｰ ⑫検収会議
運用開始	

	会議体	レビュー対象	趣旨	会議参加者（★はレビューアー）	会議時間(分)/工数(人日)	品質向上施策（会社として/個人として気を付けていること）
③	受注伺いレビュー	受注伺い書	ユーザ向けに提出する見積もりについて決裁者へお伺いを立てる	★役員 ★部門長 ★TL メンバ	60	工数や体制、基本設計内容が妥当かどうかをレビューいただく、決裁者が理解ししやすいよう工夫する。 ユーザへむけ説明する資料として流用するケースが多いのでユーザ目線もわかりやすい資料とする。ストーリに違和感がないこと。
⑤	設計書レビュー	ベンダ設計書	ベンダーの作成した仕様書や手順書が問題ないかレビューする。	ベンダ ★部門長 ★TL ★メンバ	60	以下はかならず抑える。 ・パラメータ、仕様に誤りがないか ・既存のインフラとシステム、ユーザに対してどのような影響があるか ・ステークホルダーはだれか

4. 品質向上施策のヒアリング結果分析

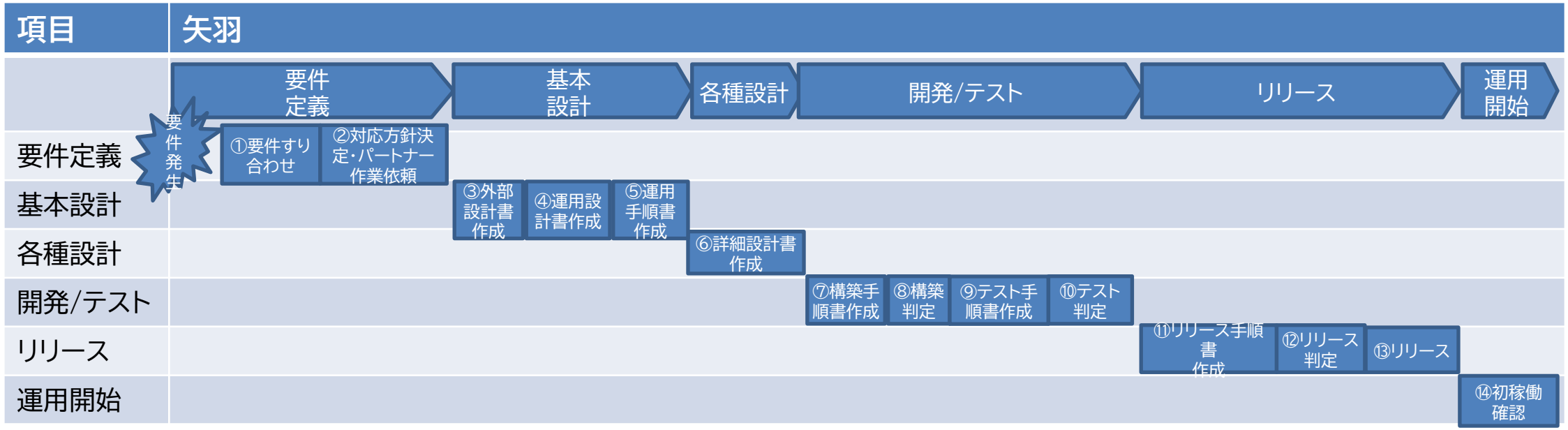
- B社(抜粋)

項目	矢羽
	要件定義 → 基本設計 → 各種設計 → 開発/テスト → リリース → 運用開始
要件定義	①協議申請 ②ベンダー選定 ③提案資料作成 ④要件定義レビュー(大規模のみ) ⑤見積・稟議
基本設計	
各種設計	⑥基本設計レビュー
開発/テスト	⑦構築・製造 ⑧テスト
リリース	⑩リリース判断レビュー ⑪ユーザーへの移行計画説明 ⑫リリース ⑬本稼働立会 ⑭評価レビュー
運用開始	

	会議体	レビュー対象	趣旨	会議参加者(★はレビューアー)	会議時間(分)/工数(人日)	品質向上施策(会社として/個人として気を付けていること)
⑥	基本設計レビュー	基本設計書	各種設計書の妥当性判断	PM メンバ	60	要件定義からの変更点 システム運用要件 方式設計(方針、システム構成、処理方式、性能設計) 運用方式、開発方式、セキュリティ方式 テスト基本計画
⑩	リリース判断レビュー	本稼働可否	本稼働できる状態か？	PM 所属長 IT部門役員	60	課題の対応状況 テスト結果(性能、障害、運用受入テスト) 本稼働体制 切戻しポイントが明確になっているか 予備日の確保 運用部門へ引継ぎ済みか

4. 品質向上施策のヒアリング結果分析

- C社(抜粋)



	会議体	レビュー対象	趣旨	会議参加者(★はレビューアー)	会議時間(分)/工数(人日)	品質向上施策(会社として/個人として気を付けていること)
⑫	変更作業チーム内レビュー	変更作業説明資料	リリースする基盤変更作業の案件を説明し、リリースの作業に問題がないか確認を行う	★チームリーダー、★ユニットリーダー、担当者	10~30分	リリースに失敗したときの影響、リリース時のサービス影響を明確にした上で、説明を行う。 リリース失敗時の影響がシステム内影響、社内影響、社外影響で影響度を確認し、社内影響以上の影響度の場合は、「変更管理リリース判定会議」へ付議することとしている。

4. 品質向上施策のヒアリング結果分析

■ サマリ

- 各社ともに品質向上施策として、各社独自の用語を用いているが、各工程でレビューを行っている。
- 開発規模が小さいものでは、レビューを省略、もしくは次工程でまとめてレビューするケースがある。
- 各社ともに大規模なシステム開発（1、000万円超）では、様々な役職の方からレビューがされている。
- 各社はレビューにより品質向上を図っていると考えられる。

  ※ レビューはステークホルダーとの合意形成という一面もあるが、本研究では品質向上の側面が大きいと捉えることとする
- レビューアーの確認観点を網羅し、上位者との意識の相違を減らすことによって、品質の向上が期待できると考えるため、前項のヒアリング結果をベースに「会議体×レビュー対象」ごとに整理。

5. 役職ごとのレビュー観点

- レビュー観点ヒアリングシート（抜粋）

会議体	レビュー対象	趣旨	部長	グループリーダー	チームリーダー	ユニットリーダー	担当者
対応方針決定	対応方針資料	・要件元からの依頼内容をもとに対応方針を担当が検討 ・その結果を上位層と合意する	・コストと得られる利益のバランスが取れているか ・体制は明確か。影響範囲となるステークホルダーは巻き込めているか ・5年換算で費用対効果があるのか ・初期費用、ランニング費用が整理されていること	・全体的な対応方針は妥当か ・要件元、関係者との調整は取れているか	・要件（ユースケース）が整理できているか ・現時点で見えているスケジュールについて、他の大規模案件と並行実施することは可能か ・誰が見ても（詳しくない人が見ても）わかりやすく、簡潔であること	・依頼内容を網羅して整理されているか ・依頼内容の目的（趣旨）にあっているか ・変更に強いか（拡張性があるか）	-
パートナー作業精緻化	・マスタースケジュール ・WBS	対応方針を受けて、パートナー社作業内容（工数含む）の妥当性を評価する	-	・リリースタイミングなどのスケジュールが妥当か ・他案件とのスケジュールの重なり有無 ・本番化してしまったらほぼできない障害試験は十分に検討されているか	・工数の根拠が適切か ・マイルストーン、クリティカルパスが明確か	・見積内容の算出根拠が妥当であるか ・対応期間にフィジビリティがあるか ・過去に同様の作業を実施している場合、習熟度による工数削減観点が考慮されているか	・スケジュールに無理がないか ・現状調査がきちんとできているか（計画されているか）
各種設計書レビュー	各種設計書（外部設計書、詳細設計書、運用設計書など）	作成した各種設計書のレビューを行う	・前回の対応内容との差分説明（対応内容、コストアップ要因） ・性能テストでは定量的な内容となっているか	・上流→下流成果物の落とし込み漏れがないか	・依頼元の要望を実現できる設計になっているか ・異常発生時の被害拡大を抑止する設計になっているか ・トラブルを起こしにくい、また起きた時に復旧し易い構成となっているか	・他システムとの整合性が取れているか確認する ・パラメータ設定値の根拠（なぜデフォルトとしているか、デフォルトでよい根拠など）	・担当外の方が見ても理解できる内容になっているか
構築手順書レビュー	構築手順書	作成した構築手順書のレビューを行う	-	-	-	・環境破壊可能性のある手順はあるか、ある場合はリスクを軽減する考慮がなされているか	・実施者の裁量になるような抽象的な手順になっていないか ・作業者が実行可能な粒度で記載されていること

5. 役職ごとのレビュー観点

- レビュー観点ヒアリングシート(抜粋)

会議体	レビュー対象	趣旨	部長	グループリーダー	チームリーダー	ユニットリーダー	担当者
構築開始判定/終了判定	・構築手順書 ・運用機能星取表 ・構築判定資料 など	・構築が開始できる準備ができているかの確認を行い、構築終了時の判定基準を確認する ・構築開始判定で定めた判定基準にしたがって、構築終了の判定を実施する	-	・構築時において発生した不備の内容(不備に傾向がないか) ・不備がある場合には類似確認などが出来ているか ・構築残課題が残っていないか ・テスト開始や次工程に向けた検証がどこまで実施できているか	・構築に向けた構築手順書やメディアなどの準備状況 ・条件付きか否か、条件付きの場合(積み残しがある場合)、それでも開始したいという理由が明確であり、条件付きで開始しても問題ないということの妥当性が確認できること	・必要な資材や手順をリストアップできているか 作業スケジュールが不測の事態も考慮しているか	-
テスト手順書作成	・テスト仕様書 ・テストケース一覧	作成したテスト仕様書のレビューを行う	-	-	・V字モデルに相応したテスト観点・テストケースが作られているか(設計書の記載・変更内容に対して、テストケースの落とし込み漏れがないか)	・テスト結果の確認/判定条件が明確になっているか(定量、定性)	・実施者の裁量になるような抽象的な手順になっていないか ・テスト実施による対外的な影響確認とテスト前との変動要素(データが更新されて問題ないかなど)
テスト開始判定/終了判定	・テスト仕様書(テストケース一覧) ・テスト判定資料 ・テストエビデンス ・テスト判定資料	・テストの開始準備、実施するテスト内容を確認し、テスト終了時の判定基準を確認する ・テスト開始判定で定めた判定基準にしたがって、テスト終了の判定を実施する	-	・テストケース種類の実施妥当性(性能テストや運用テスト、災対テストなどが充足できているか) ・テストにて発生した不備の内容(不備に傾向がないか) 不備がある場合には類似確認などが出来ているか ・テスト結果の評価は妥当か	・欠陥に対する分析ができているか ・条件付きか否か、条件付きの場合(積み残しがある場合)、それでも開始したいという理由が明確であり、条件付きで開始しても問題ないということの妥当性が確認できること	・判定基準に定めた成果物が準備できているか ・テスト実施において発生した課題が解決しているか ・不具合事象に対する原因分析と類似確認の内容	-

5. 役職ごとのレビュー観点

- レビュー観点ヒアリングシート(抜粋)

会議体	レビュー対象	趣旨	部長	グループリーダー	チームリーダー	ユニットリーダー	担当者
リリース手順書レビュー	リリース手順書	作成したリリース手順書のレビューを行う	-	-	・移行作業中のミスを極力抑える様な手順となっているか、切り戻しを考慮した手順となっているか	・影響範囲の整理ができているかどうか ・戻し手順が無理なく設定されているか ・リリース対応の体制表が準備されているか(連絡先がわかっているか) ・テスト環境と本番環境の差異を正しく把握して手順書を作成しているか	・設定変更の手順前後で変更結果が確認できる手順となっているか ・実施手順に対する確認作業が漏れていないか ・他システムやアプリ影響の調整要否などが考慮されているか
リリース判定	変更作業説明資料	リリースする基盤変更作業の案件を説明し、リリースの作業に問題がないか確認を行う	・品質懸念が残っていないか ・ユーザ部門とのリリースの調整が完了しているか ・タイムチャートが妥当か ・体制が妥当か ・コンチプランが妥当か ・リスク評価とその対策ができているか(障害が発生した場合の最大リスクは何か。その対策が検討、合意できているか。リスク分散は検討できているか) ・稼働確認の計画は万全か(アプリ部門巻き込み含めた稼働確認の網羅性、リリース前に確認できないものは初回稼働確認の計画が明確かなど)	・リリース際してリスク分散ができているか(段階的な移行などは検討ができているか) ・リリースタイミングは妥当か(月末・月初やピーク日は外しているか) ・リリースタイムチャートは妥当か(作業バッファ、問題が発生した場合の解析時間は確保できているか) ・変更に際して、関係者との連絡体制が整理・確保できているか(メーカーへの緊急連絡を含む) ・戻しを行う判断基準は明確になっているか	・各工程が既定のプロセスどおりに実施されたか ・残課題がないか(あるいはリリース後対応でも問題ないことを合理的に説明できているか) ・体制/エスカレーションパスが明確なっているか ・長時間作業や複雑な作業は途中でのチェックポイントが適切に設定されているか ・有事の戻し手順・考え方が整理されているか	・リリース判定でチェックされる項目が漏れなく実施できているか ・リリース時の制約(サービス停止など)についてステークホルダーと合意できているか ・不測の事態が発生した場合の備え(他組織メンバーの待機依頼など)は済んでいるか ・初荷確認とリリース後の体制の計画は万全か	-

6. 役職ごとのレビュー観点の分析

■ ノウハウ共有

- レビュー観点ヒアリングシートから各社で気になった点を議論し、ノウハウの共有を行った。

➢ 変更対象の影響自動分析

- インシデント管理、問題管理、変更管理をServiceNowで管理しており、変更管理においては変更対象のシステム(サービス)を入力することで、自動でリスクを評価する仕組みとなっている。
- システム(サービス)の変更による影響度合いを一元管理するものを用意すれば、変更対象の影響度合いがわかり、案件担当者判断の調整不足による障害を発生させないことができる。

➢ ナレッジ管理

- 他社ではインシデント管理、問題管理、変更管理までICDツールを利用して管理していた。
- 5社のうち2社はツールにより管理しており、他3社でもEXCEL管理をしていた。
- 全社へプロジェクト単位での実績や得られたノウハウを一覧化して共有していた。

6. 役職ごとのレビュー観点の分析

■ ノウハウ共有（続き）

➢ コマンドの妥当性・環境の保護

- システムによってはテスト環境が用意できず、作業前に実機検証が出来ない場合は、ベンダー内の疑似環境を使って検証を行うなどし、品質を担保した上で、本番環境で作業を行うようにしている。
- 削除コマンドを実行するときは、警告メッセージを表示させることを義務化させる。（使用NGと定めたコマンドリストにあてはまらないかをチェックする会社もあったが、作業負荷により形骸化した。）
- またリリース作業前には、システムバックアップを取得し、万が一不具合が発生したときに、システムバックアップからもとに戻せるようにすることで、戻し手順を含めてテストを実施する。

6. 役職ごとのレビュー観点の分析

■ ノウハウ共有（続き）

➢ ITインフラにおける品質評価

- アプリケーションのバグ密度やテストケース密度による品質評価のように、設計書やテストケースにおけるレビュー指摘件数を品質評価の指標値に入れて評価する。

  （合格条件は各会社の過去案件から定める。）

  ✓ 設計書
  設計書のページ数/レビュー指摘件数

  ✓ テスト
  テストケース数（もしくは画面数）/レビュー指摘件数

- レビューの品質担保の指標としてレビュー項目一覧等を活用して、網羅的にレビューできていることの確認をする。
- レビュー項目一覧はシステムの多様性により変動するため、社内で発生した障害対応の取り組みや最新技術等の情報に併せて最新化していく。

7. 結言

■ 結言

- レビュー観点ヒアリングの結果より、上位の役職の方々は、リリースするシステムの影響を幅広く確認し、本番業務への影響有無を重視している。
- またユニットリーダー、担当者の方々は、設計書や手順書に記載されたパラメータやコマンドの妥当性を確認することで、品質を向上させている。
- レビュー観点の分析より、各工程の基本的な部分がおろそかにならないようにすることが最も重要だと考える。
- 当グループでは以下の3つを再度自社に持ち帰り、強く共有することとした。

  ① システム(サービス)の変更による影響度合いを一元管理するものを用意し、変更対象の影響度合いを判断ができる仕組みを用意する(ツールの使用等検討する)。

  ② レビュー項目一覧を陳腐化させないように、社内事案や最新技術の情報を取り込み、最新化する。

  ③ 上位者レビュアーの観点を資料の中に明記できるように取り組む。
  (上位者との意識の相違をできるだけなくせるようにする)

8. 活動感想コメント

■1年間ありがとうございました。このような活動に参加するのが初めてで、かつリーダーという立場で研究を推進していく経験は、自分自身の成長に繋がったと思います。貴重な機会をいただきありがとうございました。

23年度は業務の中で品質とはなにか？を考える機会があったため、とても有意義な活動となりました。研究の中で学んだ品質向上施策について、自社に持ち帰ろうと思います。

■本活動をきっかけにして、普段直接お話をする機会のない立場の方からレビューとは、品質とは何かについてお考えを伺うことができました。

また他社の様々な立場の方と品質についての意見を交換することができ、1年間の研究会を非常に有意義に過ごすことができたと思います。

■1年間、皆様と共に研究活動に参加できたことを大変うれしく思います。

研究テーマに関わらず、他社の利用しているツールやどんな手順を踏んでリリースを行っているのか、利用している背景や事情、似たような悩みを抱えていることが分かりアドバイスをいただいたり、逆に自社の事例を紹介することができ貴重な体験となりました。

担当者、リーダー、プロジェクトリーダーなどの立場や職務内容に関わらず意見交換でき大変有意義な活動だったと考えます。

自分自身、また機会があれば次回以降も参加させていただきたく、また、自社に持ち帰り本研究内容を共有するとともに別の担当にも自信をもって進められるものとなりました。1年間、大変お世話になりました。

8. 活動感想コメント

■JUAS運営、幹事団の皆様、研究会メンバーの皆様1年間ありがとうございました。

私自身普段、社外の方と交流する場がほとんどなく、最初は大変緊張しておりましたが、実際に色々なインフラエンジニアの方とお話してみて、共感できることも多く、大変打ち解けることができたと思っております。

今回分科会活動としてインフラの品質向上施策を研究しておりましたが、施策として他社様ではどのようなことをしているか、どういった運用をしているのか知ることができ、また議論することができ、私自身成長することができた時間だったなと感じました。

もちろん分科会活動だけでなく、お悩み相談会等の研究会活動を通して学ぶことが多かったと思っております。

今回の研究会活動を通して取り組んできた内容はぜひ社内へ持ち帰り、社内展開したいと考えております。

■社外の方々と交流、意見交換をさせて頂くことで視野を広く考えられるようになり、貴重な経験となりました。

1年間ありがとうございました。

2023年度 ITインフラ研究会
分科会5　活動報告資料

業務標準化を目的としたAIによる自動ドキュメント化

2024年4月

分科会5

プロジェクト背景とテーマの選定理由

【背景】
・インフラ人員の離職や業務属人化により、インフラ業務の継続性という観点から、各社類似の課題。
・業務標準化、引継ぎの簡素化が重要。
・標準化・簡素化するにはドキュメント作成にかける時間を確保することが困難。

これらを解決する方法は？

普通にドキュメント作成をしてもおもしろくない・・・

AIを使って、ドキュメントを自動で作成すればいいじゃない！！

自動化と業務標準化への取り組み

■手順書作成が進まない理由・・・「手順書の作成に割く時間と意欲がない。」という考えが根底にある

アンケート結果
:Q　なぜ手順書がないですか？
　A　手順書を作っている時間がないから
　　手順書を作るほど難しい業務ではないから
　　手順書としては作成していないが自分専用のメモレベルならある

簡単に手順書を作成できる方法を見つけることで課題の解決に繋げる

人力での作成には労力がかかるが、
「AI」を活用することで効率的にドキュメント作成ができるのではないか？

AIツールMicrosoft Copilotの機能紹介

Microsoft Copilotとは、Microsoft 365に組み込まれたAIツール
M365ユーザーの生産性を向上させるための様々な機能を持つ

＜機能＞
- Copilot in Teams：会議やチャットなどの要約やインサイト提供
- Copilot in Outlook：メール作成、スレッドの要約
- Copilot in Word：ドラフトの作成や校正
- Copilot in PowerPoint：既存ファイルやプロンプトなどからのスライド作成など
- Copilot in Excel：既存シートからの傾向分析やデータビジュアライゼーションの作成など

今回はCopilotで検証！

（理由）
- ドキュメント生成＝Office製品のイメージ
- 23年のタイムリーな話

⇒興味と話題性を重視
（明確な根拠があるわけではない、、、）

＜活用のポイント＞
- 各Officeアプリケーション上での実用性を見極める
- 資料のドラフト作成を行う際は、あくまでアシストツールの一つとして、最終的なチェックは人が行う

＜活用シーン＞

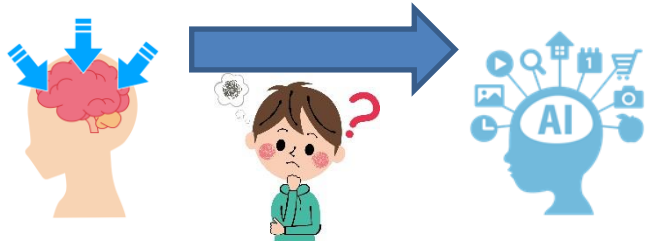
Word、PowerPointでの資料作成、Teamsやメールでのコミュニケーションなど、Microsoft 365で行う業務全般のアシスト

検証方法

まずはインプット情報をどのようにとりこむか？

手順は頭のなかにある

頭のなか ⇒ AIへインプット



インプット方法検討

効率化！！

案	きれいでなくてもいいから、頭の中の情報を書き起こす ⇒手順書として、生成AIで整えてもらえばいいのでは？？	書き出しすることが困難であれば、話してもらえばいいのでは？ ⇒話した内容を書き起こす部分を生成AIに任せる
評価	**【やる意義は少なそう】** ＜アンケート結果＞ ・書き起こす作業自体が手間・時間取れない ＜先行導入メンバーからの参考意見＞ ・統一した成果物が出来上がるわけではない ・整えるためのプロンプト作成が困難 （プロンプト作成のための手順書用意、といった矛盾にも繋がるかも）	**【なんか形にできそう】** ・CopilotはTeams会議の議事録作成が可能 ⇒議事録ではなくて、手順としてまとめてくださいと指示すればいいのでは？ ・手を動かす（手順書作る）のは面倒だけど、話すのは手間ではないのでは？ ⇒口頭引継ってよくあるよね？という会話から。 ・つい口頭引継しがちなものを、まずはドキュメントとして残せたらよいのでは？ ⇒後任のこと考えると、何もないよりは少なくともプラスなはず。

検証方法の具体化

Teams会議で手順の口頭説明を行い、文字起こし機能（トランスクリプトから）使って文書化する！

検証結果からみる実践可能性

GOODポイント

- 会議内で説明した手順に対して、copilotの要約精度は高い
  - 各担当共に、説明時間は長くなったものの、手順としてはほぼ**漏れなく**まとまっている
  - 注意事項など、手順だけでなく、補足情報も取込される
- 実際に手順・注意事項として発言していない内容も、一般論として注意すべき観点の補完あり

BADポイント

- Officeファイルへのアウトプットとしては、実用的に使用することはできない
  - 手順をテキストレベルで残すには充足するが、Officeファイルとしての整備は困難な印象
- 音声データのみからテキスト作成のみに留まる（説明に使った際の画面イメージ・資料は別途作成必要）
  - 例としては、画面を使った操作説明の場合、このボタンを押下するなどあるが、画像キャプチャと手順が一緒に残されていた方がわかりやすいが、手順のみしか残せない、といったイメージ。

使えそうな場面の想定

口頭で業務引継を行う場合

・引継先のメモに頼り　⇒　引継元・先双方で認識相違ないか確認可
・俗人化・知識のブラックボックス化　⇒　視える化

ベテランからのノウハウを引き出す場合

・教えてくださいと聞けば、話してくれる（ドキュメント化よりハードル低い）
⇒話した内容を（Copilotで）書き起こすことで視える化

※いずれの場合もOfficeファイルへのアウトプットなど高度なレベルはまだ求めてはいけない（テキストベースで手順・ノウハウを残すイメージ）

AIツールのさらなる進化への期待

・Copilotは会話や文章の要約することには秀でている
　└要約されすぎないような注意は必要。（プロンプト作成するのに苦労する、、は避けたい。）
・今回の目的としていた手順作成用途としては、以下を期待したい

＜画面キャプチャの取得＆書き出しファイルの選択肢拡充＞

【インプット】
　録画データとトランスクリプト
【アウトプット】
　・手順の説明時、「画面ハードコピーを取得」などキーワードに
　　録画データ用いて、画面ハードコピー取得。
　・画面ハードコピーとテキストを合わせて、手順として書き出し
　・書き出し先ファイルとしては、Excelやwordなど指定したファイル形式で出力

【補足】
※今回の議論では、信頼性や安全性に関する課題については議論の中で取り上げていない。
※メンバーのPCでCopilot導入PCがなかったので、トライ&エラーを繰り返せなかった点は反省点。
（AIをテーマに活動する際には、自身で動かせる環境構築が推奨）

2023年度 ITインフラ研究会
分科会6

ITインフラの事業継続計画について

2024年4月

分科会6

目次

1. BCPとは(1/2)

事業継続計画(BCP:Business Continuity Plan)
災害時に特定された重要業務が中断しないこと、また万一事業活動が中断した場合に目標復旧時間内に重要な機能を再開させ、業務中断に伴う顧客取引の競合他社への流出、マーケットシェアの低下、企業評価の低下などから企業を守るための経営戦略。
※内閣府　防災情報のページより(知る・計画する：防災情報のページ - 内閣府 (bousai.go.jp))

上記の記載通り、事業を継続させるための対策であり、
災害以外にも、テロやシステム障害、不祥事といった危機的な状況に置かれた場合に重要な業務を継続させるための方策を示す。

1. BCPとは(2/2)

BCPを行う目的は大きく分けて「緊急時の事業の継続・早期復旧」と「社会・顧客からの信頼性向上」の二つがあります。

①緊急時の事業の継続・早期復旧
BCPを策定する一番の目的は、緊急時における早期対応です。緊急時には事業継続に深刻な影響が出ることによる業績低下や、できる仕事がないために従業員が働く機会を失い、最悪の場合はリストラの可能性も出てきます。緊急時でも事業の核となる部分は継続させるなど、早期復旧が求められます。

②社会・顧客からの信頼性向上
副次的な効果として、BCPを策定することで、災害時への対策をしているというパブリックイメージの向上につなげられます。自社の事業の継続性だけでなく、非常時の社会貢献などの活動も項目に置けば、CSR活動としても良いイメージを醸成することが可能です。

2. BCPの取り組みの現状(1/2)

令和3年度介護報酬改定(厚生労働省)
3年間の経過措置期間後である令和6年度(2024年4月)より、全ての介護サービス事業者を対象に、業務継続に向けた取り組みが義務化

一方、その他の民間事業の事業継続計画は自主的な取り組みの推奨に留まっており、自然災害を対象とした事業継続マネジメントのガイドラインを内閣府にて作成・公開
※内閣府　事業継続ガイドライン(https://www.bousai.go.jp/kyoiku/kigyou/keizoku/sk 04.html)

2019年度調査でも事業継続計画策定のきっかけは「リスクマネジメントの一環」が約30%と一番高く、各民間企業の自主的な取り組みの割合が高い
※内閣府　令和元年度企業の事業継続及び防災の取組に関する実態調査
(https://www.bousai.go.jp/kyoiku/kigyou/topics/pdf/r2 gaiyou.pdf)

2. BCPの取り組みの現状(2/2)

2023年度調査では事業継続計画に取り組む意向がある(計画済みを含む)が過半数を下回り、事業継続計画の策定率も毎年右肩上がりではあるが、中小企業で2割程度、大企業で4割程度と市場全体でみると依然として取り組めていない企業が多い

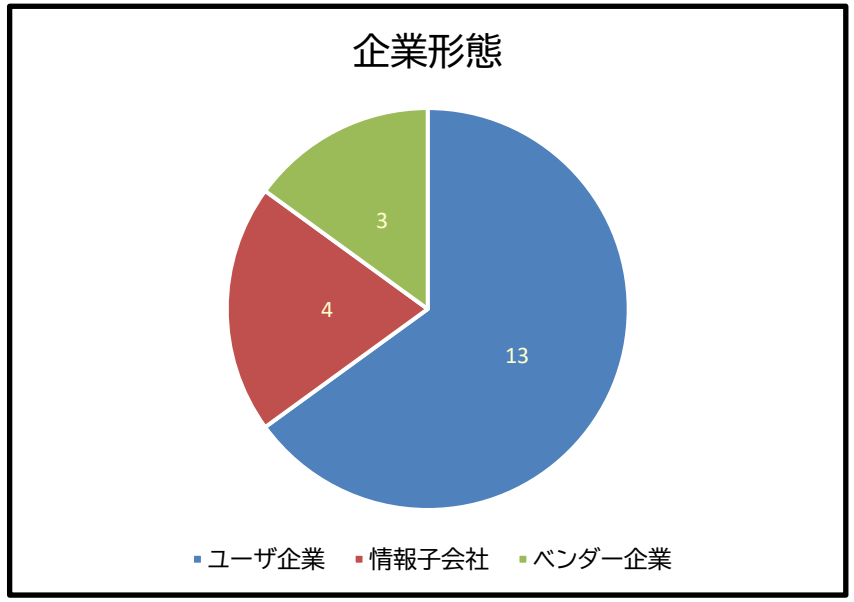
事業継続計画の策定に取り組めていない理由には

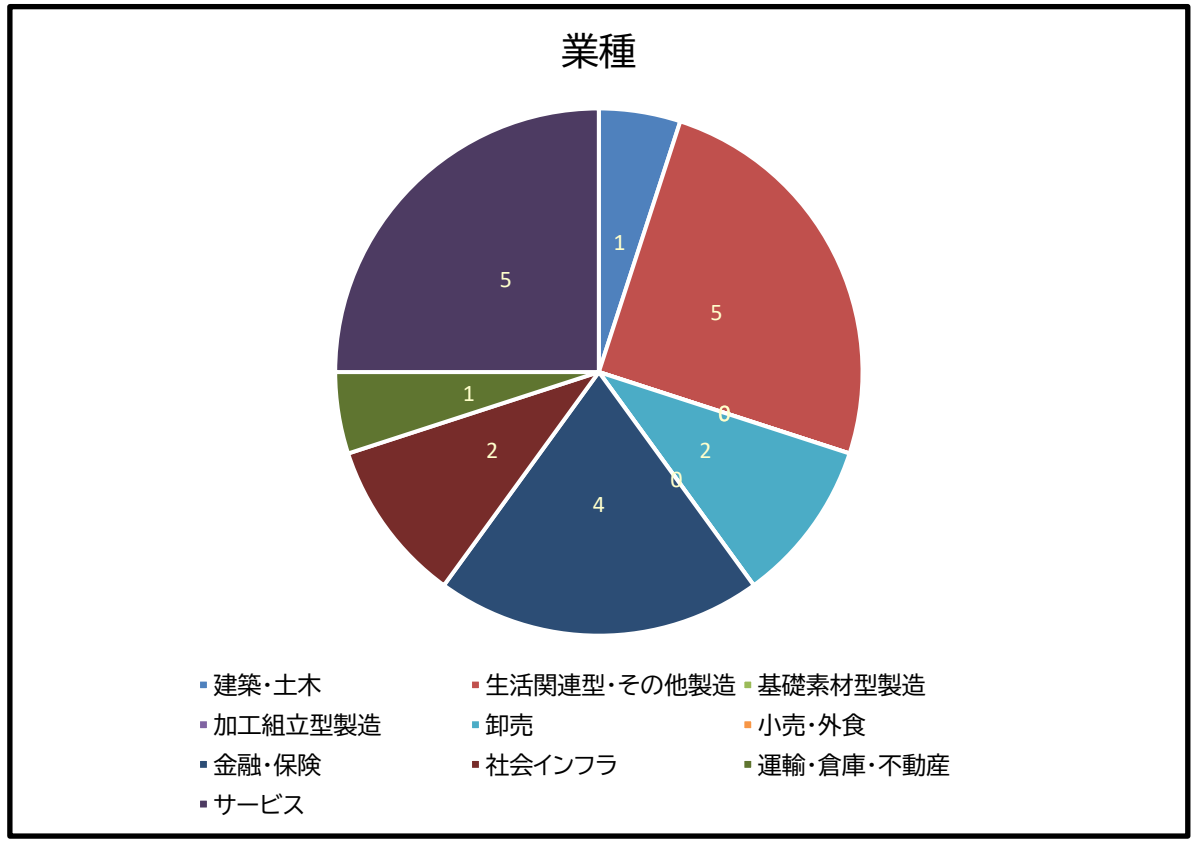
・事業継続計画を策定できる人的リソースおよび
　他の業務との兼ね合いによる時間的リソースの確保が難しいこと

が主要因としてあげられており、事業継続計画策定に取り組むにあたって、その手段/対象範囲/どこまで検討をすれば十分かの判断ができないといったナレッジ・スキルが不十分であることが推進が進められない要因の一つと判断できる

3. BCPに関するアンケート(1/6)

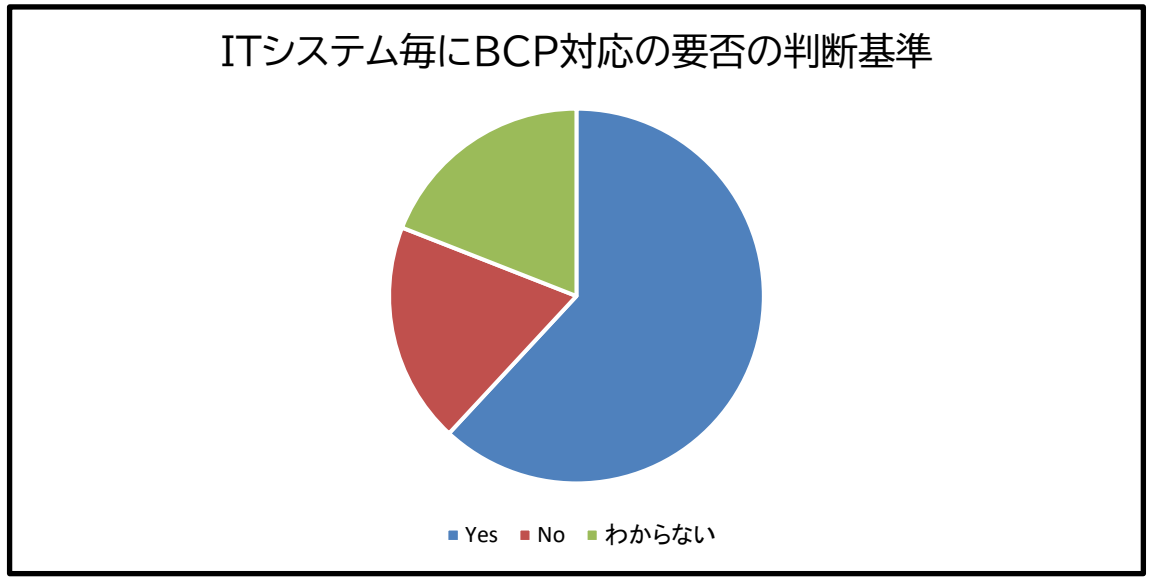
アンケート実施時期:2023年12月
アンケート回答会社:21社
（ITインフラ研究会参加企業）





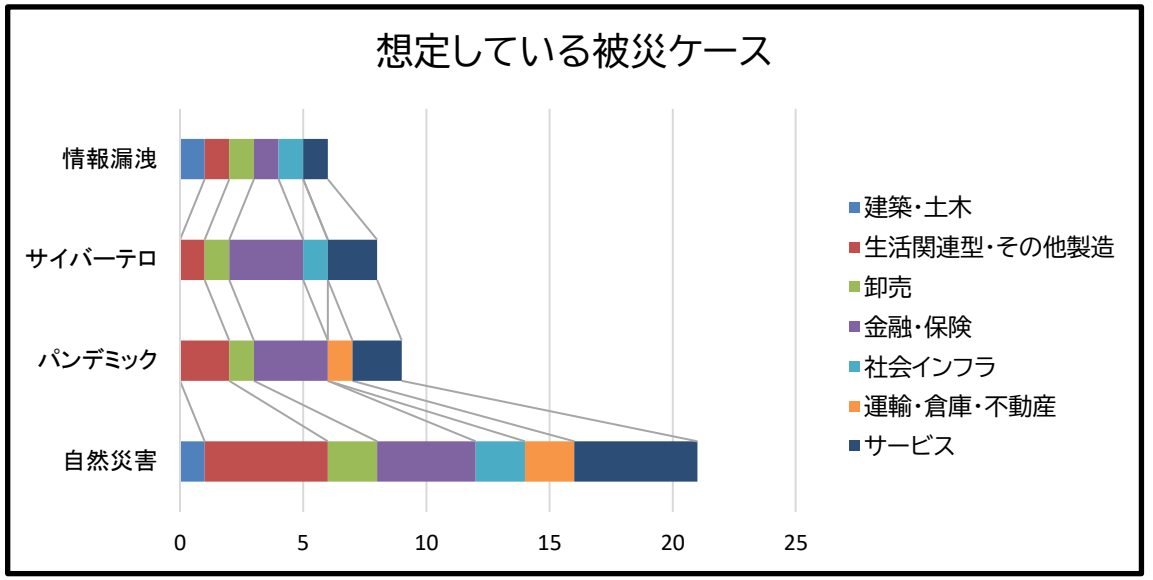
3. BCPに関するアンケート(2/6)

ITシステム毎にBCP対応の要否の判断基準



- **明確なBCP対応を判断基準がないという回答が約20%**あった
- 各被災パターン(関東、関西広域被災、拠点被災など)ごとに各システム対応要否がるという回答もあった
- **ポイント制で対応レベル判断**している回答もあった

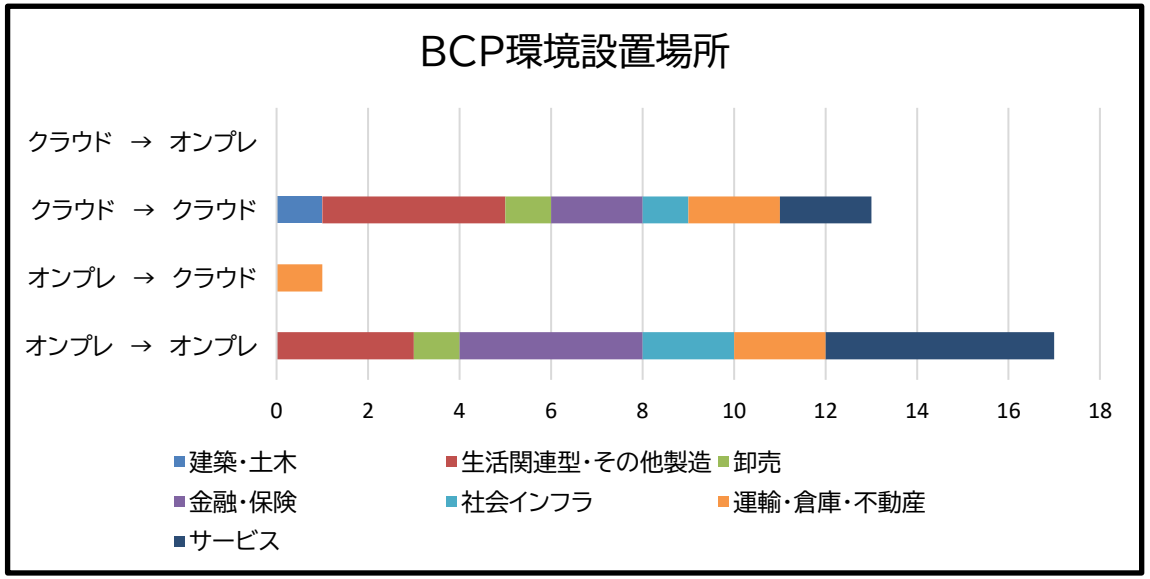
想定している被災ケース

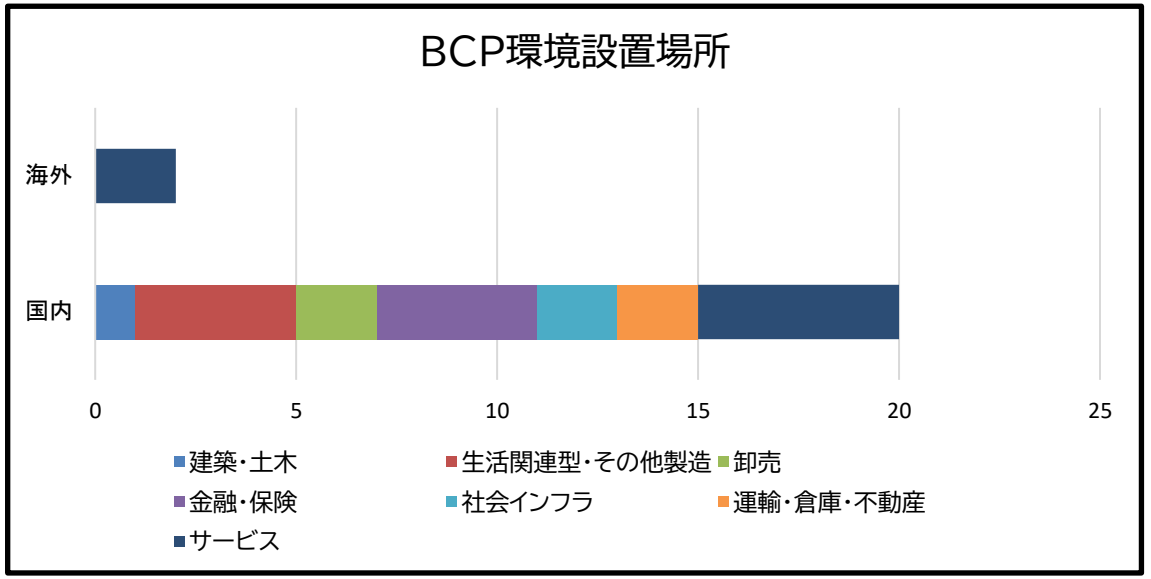


- **各社"自然災害"は想定**しており、約4割の企業が"パンデミック"と"サイバーテロ"についても対応している

3. BCPに関するアンケート(3/6)

BCP環境の設置場所



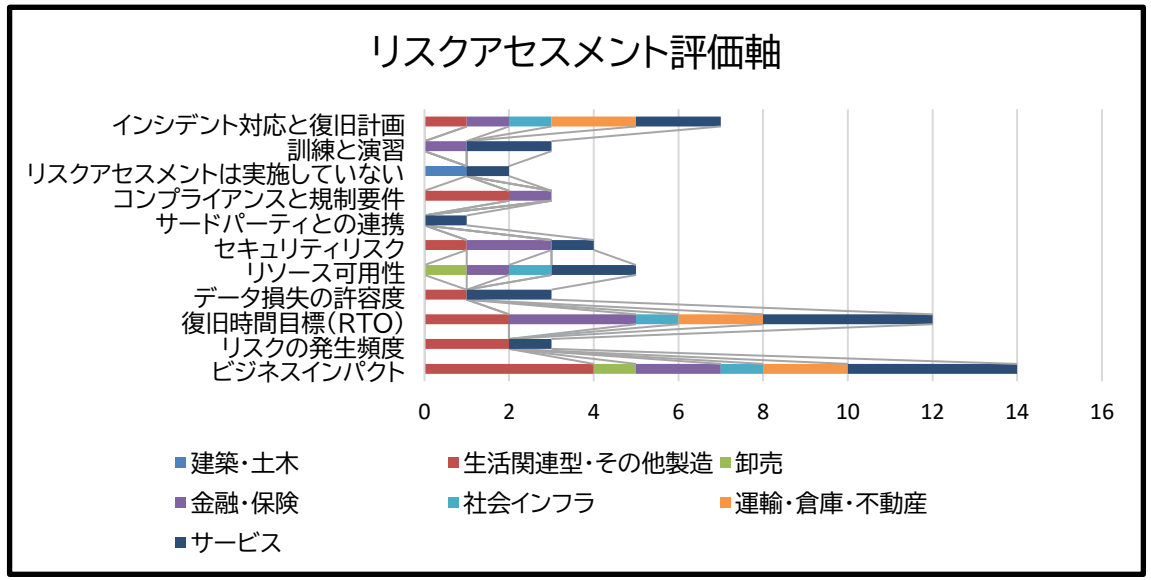


- 8割の企業がオンプレのBCP環境に設置
- オンプレからクラウドのBCP環境への設置は1企業のみだった

- BCP環境は国内設置が大半を占め、海外にへの設置は2企業のみだった

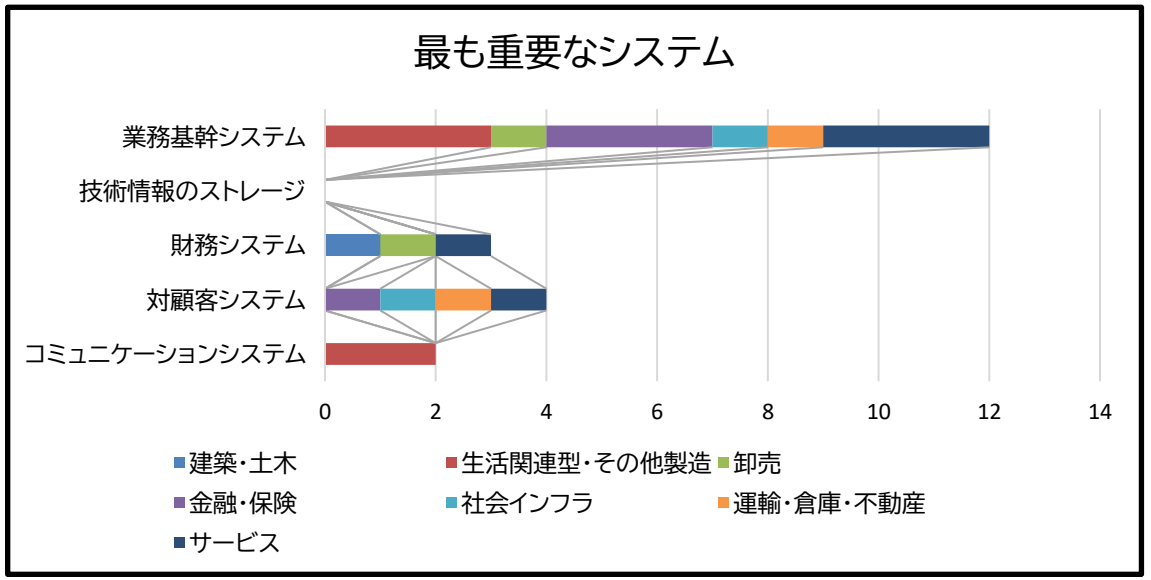
3. BCPに関するアンケート(4/6)

BCPリスクアセスメントの評価軸



- 8割の企業が、ビジネスインパクトとなり、6割の企業でも、復旧時間目標となった。
- 1割の企業がリスクアセスメント未実施となった。

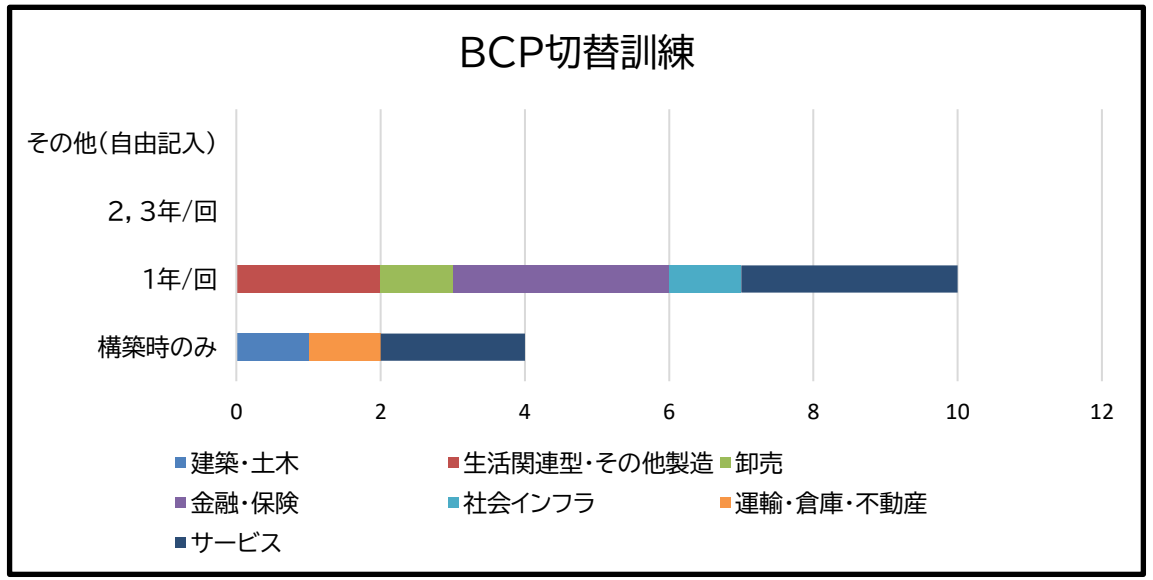
最も重要なシステム



- 半分以上の企業が”業務基幹系”を選択
- ”コミュニケーションシステム”は”生活関連型・その他製造”企業のみが2社選択

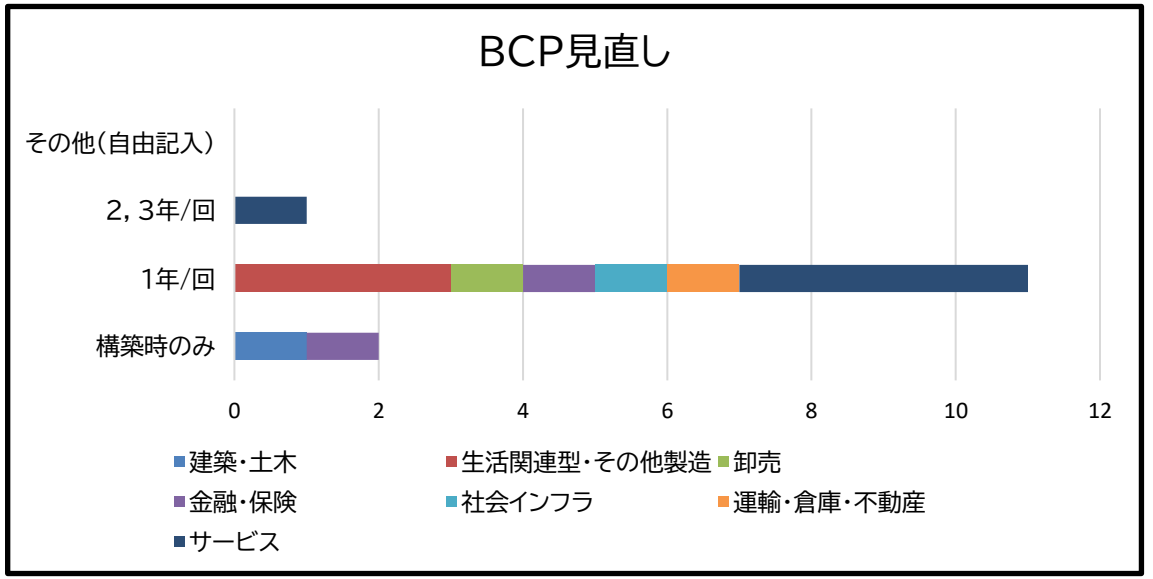
3. BCPに関するアンケート(5/6)

BCP環境の切替訓練



- 5割の企業が、年1回の切替訓練を実施している
- 3割の企業が、訓練未実施となった

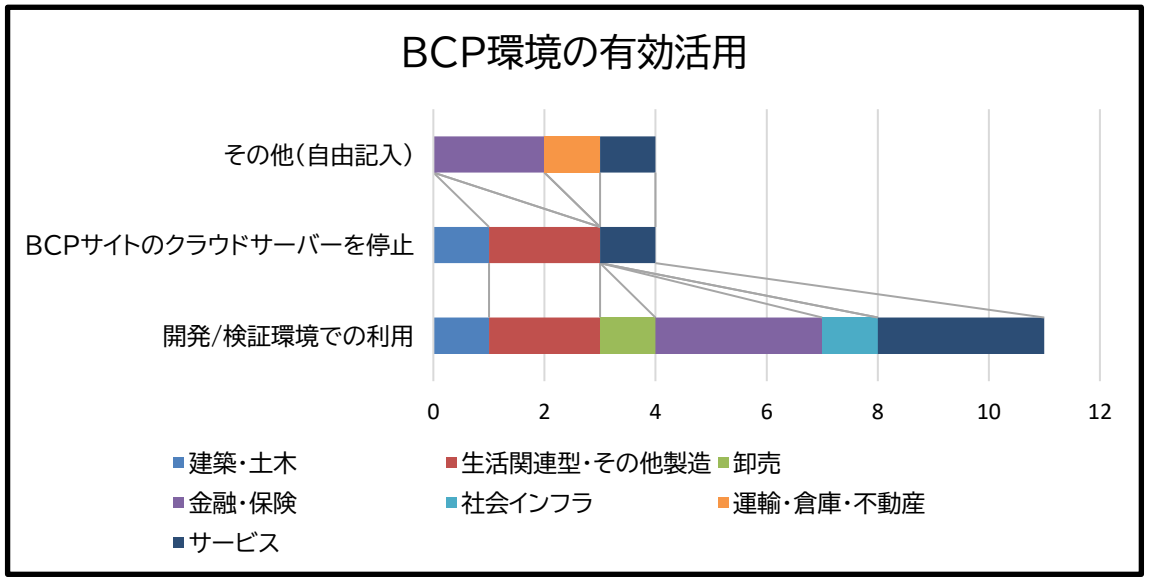
BCPの定期的な見直し



- 5割の企業が、年1回の見直しを行っている
- 訓練に合わせて見直しているという意見があった

3. BCPに関するアンケート(6/6)

BCP環境の有効活用



- **5割の企業が、BCP環境を開発/検証環境で利用**している
- その他、定期的な交互運用やBCP環境を冗長環境での利用している意見もあった

4. 検討時の課題、注意点のまとめ(1/2)

アンケートから「BCP検討時に困ったこと」

1. 費用対効果に関すること
   (1)**どこまで予算をかけて、どこまで対象にして良いのか決めるのが難しい**
   (2)**効果を求める業務部門とシステム部門とでBCP対策に温度差**があり、費用対効果の調整に苦慮した

2. 計画の精度に関する不安
   (1)計画が十分なのか明確になっていない
   (2)計画に十分なスキルの有るメンバー限られている
   (3)**切り戻しの計画が十分でない**こと

3. その他
   (1)**マルチクラウド化により個別の切り替え検討**が難しい
   (2)**クラウドシフトにより基準の見直しに手間**がかかっている

4. 検討時の課題、注意点のまとめ(1/2)

アンケートの「BCPの課題」

1. 実効性に関する課題
   (1)システム単体でBCPを行っているが、**業務観点で検討されていない**
   (2)構築時に災対テストは行っているが、**本番同等のデータで訓練を行っていないため想定通りに切り替えられるかが課題**

2. 運用負荷の課題
   (1)個別システムと基盤系など共通システムが**システム毎に通常かDRかを判断し制御するのか難しい**
   (2)システムにより拠点が離れているので管理がしにくい

3. その他
   (1)**SaaSサービスのバックアップ環境の準備**
   (2)災対環境で計上した情報を、**通常系回復後に、情報反映させるのが困難**
   (3)既存システムのアップデートと災対訓練まで間が空いてしまい災対切替の品質維持が難しい
   (4)**被災時の社内へ連絡・周知手段の確保**。代替連絡手段をどの程度用意しておくのか。
   (5)東京の人員は無事である想定で計画している

5. 考察(1/3)

1. JUAS参加企業21社にアンケートを依頼した結果(質問4)、21社中20社(95%)がIT-BCPの取り組みをしていると回答があった。
⇒大多数の企業でIT-BCPの取り組みが必要と理解している事が分かった。

2. IT-BCPの対応要否の判断基準を確認した結果(質問6)、13社(62%)がYesと回答、4社(19%)がNo、4社(19%)が分からないと回答があった。
⇒半分以上の企業が危機対応マニュアル、拠点やシステム毎の重要度評価などの判断基準があると回答したが、半分弱はNoや分からないと回答した事より、何らかの事情(経営陣の関わり、コスト、業務の重要度など)により、企業の取り組み方が十分では無いと推測される。

3. 想定している被災ケースを確認した結果(質問7)、21社(100%)が自然災害と回答、パンデミックやサイバーテロは約40%、情報漏洩は約30%であった。
⇒想定している被災ケースとして自然災害は全てとなっていたが、約40%がパンデミックやサイバーテロのケースを想定していた。これは、2019年12月の新型コロナウイルス(COVID-19)の流行や昨今のサイバーテロの増加などを反映したものと考えられる。

5. 考察(2/3)

4. BCP環境設置場所の環境を確認した結果(質問8)、オンプレ→オンプレが17社(81%)、クラウド→クラウドが13社(62%)であり、その他はオンプレ→クラウドが1社(5%)のみであった。
⇒BCP環境は現在の環境をそのまま設計する傾向が大きく、環境を同じにした方が設定の面で簡単であるためと考えられる。
また、クラウドよりオンプレの方がよりBCP環境を必要と考えている傾向があった。クラウドの方がオンプレより安定動作している、環境が古い、基幹システムが稼働しているからでは無いかと推測される。

5. BCP環境設置場所の国を確認した結果(質問8)、国内が20社(95%)、海外が2社(10%)であった。
⇒現状は国内環境でのBCPを中心に考えており、費用や規則などの関係かと推測される。

6. リスクアセスメントの評価軸を確認した結果(質問9)、14社(67%)がビジネスインパクト、12社(57%)が復旧目標時間(RTO)を重視している事が分かった。
⇒災害発生時に、重要システムを早急に復旧させて、業務に影響が出ない事を重視している事が分かる。

5. 考察(3/3)

7. 最も重要なシステムを確認した結果(質問10)、業務基幹システムが12社(57%)、対顧客システムが4社(19%)と続いた。
⇒ビジネスインパクト回避のため、業務基幹システムを最重視している事と、顧客向けシステムを重視している事が分かった。

8. BCP切替訓練を確認した結果(質問11)、10社(48%)が1回/年、構築時のみが4社(19%)と続いた。
　また、BCPの定期的な見直しを実施しているかを確認した結果、11社(50%)が1回/年、構築時のみが2社(10%)と続いた。
⇒約半分の企業が1年に1回BCP切替訓練と見直しを実施している事が分かった。その他半分は構築時のみか未実施となっていた
　環境によってBCP切替訓練が出来ないという意見もあった。

9. BCP環境の有効活用を確認した結果(質問13)、11社(50%)が開発/検証環境での利用をしており、4社(19%)がBCPサイトのクラウドサーバーを停止(課金停止)していた。
⇒約半分の企業でBCPサイトの有効活用やコスト削減等に取り組んでいる状況が分かった。

6. まとめ(1/2)

1. 導入時の注意事項
   (1)体制
   経営主体で進めたいが、主管部門を設けて関係部門(経営企画、人事、総務、IT、業務部門など)を巻き込んで体制を構築しましょう

   (2)対象業務
   ・対象となる中核システムと復旧時間を明確にしましょう
   ・想定する被災ケースを明確にしましょう

   (3)予算
   BCPは企業の存続に関わる問題のため、議論を費用対効果ではなく経営課題としてとらえて予算を確保しましょう
   上記(1)、(2)を決めてから予算を検討しましょう

6. まとめ(2/2)

2. 運用時の注意事項

(1)体制

想定する被災ケースにあった連絡体制、人員配置(※)になっているかを確認しましょう

※BCP発動時の操作権限

(2)訓練および見直し

・年1回の実施が望ましい

・環境的に難しい場合は開発環境や机上でも実施することが望ましい

(3)通常運用

DRサイト側のメンテナンス指針決めておきましょう

(データ/設定同期、脆弱性対応)

(4)DR環境の有効活用

開発/検証環境での利用やクラウドの場合はサーバ停止によりコストを削減しましょう

⇒ 今後構築するシステムはクラウドネイティブなシステム構築しましょう

メリット:構築時、運用時におけるコスト