2024年度 ITインフラ研究会
活動成果報告

2025年4月

ITインフラ研究会

2024年度 ITインフラ研究会　～分科会テーマ～

分科会A	プラットフォームの値上げはチャンスか？ベンダーロックインを乗りこなせ！
分科会B	DXを実現するデジタル技術：AI活用の深化
分科会C	CIS Controlsを用いたセキュリティレベル向上ケーススタディ
分科会D	ITインフラの適切な維持、管理に向けた運用設計の研究

2024年度 ITインフラ研究会
分科会A　活動報告資料

プラットフォームの値上げはチャンスか？
ベンダーロックインを乗りこなせ！

2025年4月

ITインフラ研究会　分科会A

目次

1. はじめに
①テーマ選定の背景と目的

■2023年から2024年にかけて、VMwareのライセンス変更が発生し、多くの企業にとって
コスト増など、今後の仮想化市場や利用している企業に大きな影響を与える可能性が発生した

■多くの企業が利用しているスタンダード製品のため、多くの担当者も対応に困っているのでは？

目の前の困った・・

- 企業はどんな対策をしたのかな？
- 今回の値上げで影響を受けなかった企業はあるのか？
  あるとしたらどのような特性を持つ企業なのかな？

今後は・・

- 今回の問題をうまく解消できたとしても、**再発リスク**を解消するにはどうしたらいいのかな？

1. はじめに
①テーマ選定の背景と目的

本発表の目的

各担当者の検討の参考となるような情報を提供したい！

■VMwareの価格改定への各社の対応や、今後のVMware利用方針を知見として共有する

■どのようなシステム構成がベンダーロックインによる悪影響を回避しやすいのかを示す

1. はじめに
②本発表の概要

ベンダーロックインとは何か？

なぜベンダーロックインは起こるのか？

アンケート内容と集計結果

アンケート結果からわかること

提言

- ベンダーロックインを発生させないためにできること
- 「クラウドロックイン」にご用心
- ベンダーロックインを乗りこなせ！

2. 報告内容
①ベンダーロックインとは何か？

ベンダーロックイン	特定ベンダーの独自技術に大きく依存した製品、サービス、システムを採用した際、 他ベンダーへの乗り換えが困難になる現象のこと

■主な原因1
システム仕様が不明瞭

他のプラットフォームにシステムを拡大したい。
でも現行システムの設計書が古いままで、稼働するかわからない、、、、、

■主な原因2
ベンダーの契約期間の影響

来年までにシステムを他社サービスに移行したい。
けど、3年間のライセンス契約を結んでいるから移行後もライセンス費を払わなくては、、、、、

2. 報告内容
①ベンダーロックインとは何か？

■ なぜVMWare製品にロックインしてしまったのか？

- VMwareは仮想化ソフトウェアの、世界シェア80%以上と圧倒的なシェアを誇る。
- エンタープライズ利用では高い信頼性が求められるため、長く業界トップを走るVMware一択となっており、ベンダーロックイン状態となっていた。

■ 時系列でのシェア拡大の概要

年	バージョン	主な特徴
2001年	VMware ESX 1.0	初の商用バージョン。ハイパーバイザーとして仮想化の基盤を提供。
2007年	VMware ESX 3.5 / ESXi 3.5	ESXi(軽量化されたハイパーバイザー)が初めて登場。
2009年	VMware vSphere 4.0	ESX/ESXi 4.0。初めて「vSphere」という名称が使用される。
2011年	VMware vSphere 5.0	VMFS 5の導入、最大32台のvCPUに対応した仮想マシン、vSphere Web Client登場。
2012年	VMware vSphere 5.1	SSO(Single Sign-On)、vSphere Replicationを追加。
2013年	VMware vSphere 5.5	vSANプレビュー、最大62TBの仮想ディスク対応、vFlash追加。
2014年	VMware vSphere 6.0	vCenter間のvMotion対応、vSAN完全統合、最大128台のvCPUに対応。
2016年	VMware vSphere 6.5	HTML5ベースのvSphere Web Client、暗号化機能、VCSAの機能強化。
2018年	VMware vSphere 6.7	vSphere Client(HTML5完全対応)、パフォーマンスの最適化、vSphere Platinum導入。
2020年	VMware vSphere 7.0	Kubernetesとの統合(vSphere with Tanzu)、Lifecycle Manager、セキュリティ強化。
2022年	VMware vSphere 8.0	vSphere Distributed Services Engine(DPU対応)、NVMe over TCP対応。

1. 2008年頃: 市場の黎明期
   - VMwareはESX(i)を提供し、仮想化技術の先駆者として市場をリード
   - Microsoft Hyper-V(2008年リリース)はWindows Serverとの統合を強調して参入
   - Citrix XenServerはオープンソースの Xenプロジェクトを商用化し競争
2. 2010年代初頭: 仮想化の普及と競争の激化
   - VMware vSphereは性能、安定性、エンタープライズ機能(vMotion、DRSなど)で優位性を確立
   - MicrosoftはHyper-Vの機能強化を進め、コスト面で中小企業を中心にシェアを拡大
   - Citrix XenServerは無料化戦略を展開するも、市場シェアの拡大には至らず
3. 2010年代中盤: 市場の成熟
   - VMwareがvSphere 6を発表し、vSANやNSXなど仮想化以外の統合機能を強化
   - Hyper-VはWindows Serverの普及と共に堅調なシェアを維持
   - Citrix XenServerは市場での存在感が低下、企業向けのフォーカスにシフト
   - OpenShift(2014年リリース)はコンテナ仮想化の台頭で注目を集め始める

2. 報告内容
①ベンダーロックインとは何か？

■なぜVMWareは日本で独占的なシェアに至ったか？

- VMwareは**競合他社・製品と比較して、(日本においても特に)サポートや信頼性が高い**
- 「Broadcomによる買収以前、VMWareは我々との距離感が非常に近く、エンタープライズ領域のプラットフォームとして利用するという点において、圧倒的な信頼感があった。」

■ 親しみやすい技術情報と寄り添ったサポートでユーザーの信頼を獲得

- 日本人技術者の手によるわかりやすい技術資料
- 手軽に直接VMware技術者と対話でき、現場の声を反映したセッション

■ 活気のあるコミュニティ活動を通じ、熱意あるファンを獲得し支持者に

- 積極的なユーザー研究会、業界内のIT技術者の交流会等のイベント
- ITインフラのディファクトスキルセットとしての資格認定

Broadcomによる買収以降で
これらがひっくり返ったので、衝撃

企業のIT部門にフレンドリーな施策により緊密な関係を構築

2. 報告内容
①ベンダーロックインとは何か？

デメリット	メリット
1. ベンダーに左右されやすく、品質の低下を招く 2. 他社製品、サービスへの移行が難しくなる 3. システムの老朽化を招く	1. ベンダーのサポートの質が向上する 2. システムの統一が可能 3. スケールメリットが享受できる

ベンダーロックインは、
デメリットに着目されやすいが、
企業の状態によっては、
メリットを享受できることもある

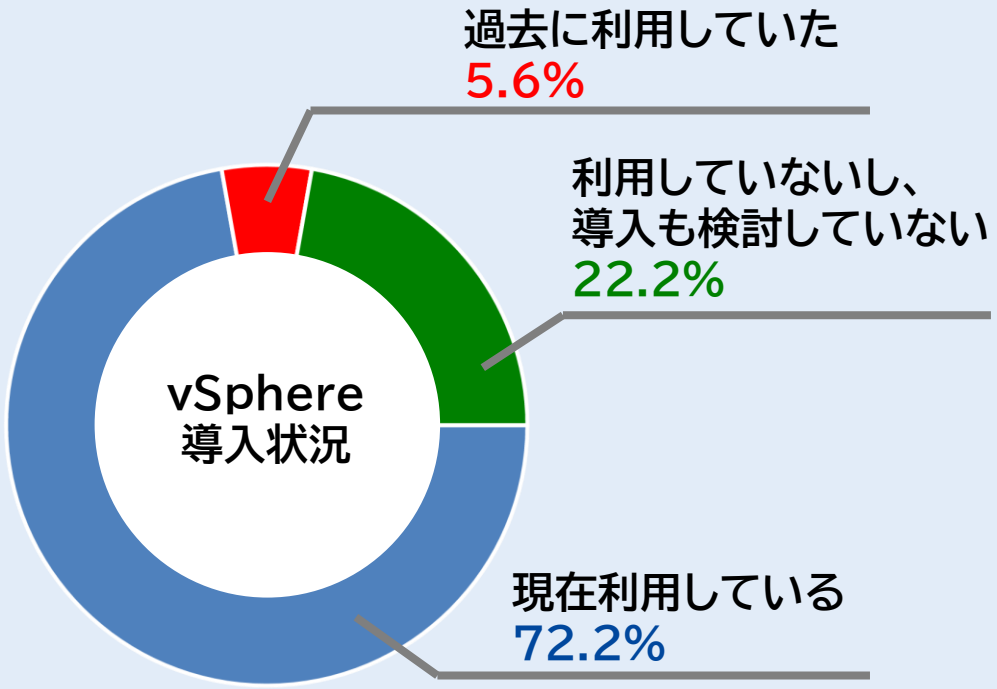
2. 報告内容
②-1アンケート概要と結果

■ アンケート調査の概要

アンケート実施の目的	• VMwareの買収を実例として、企業におけるベンダーロックインの現状を把握する • VMware買収を契機に、企業のIT基盤や仮想化戦略がどのように変化したか、またその影響をどのように受けているかを分析する • 現状のvSphere導入状況、ライセンス形態の変化、直近のライセンスコストの動向を通じ、企業がどのような対策を講じているか、今後のクラウド化戦略や他プラットフォームの検討状況を明らかにする • 調査結果をもとに企業が直面するベンダーロックイン問題への具体的な対策や、将来の技術選定に必要なインサイトを提供する
主な質問内容	• vSphereの導入状況 • 23年度と24年度のライセンスコストの変化 • 中長期的なITインフラ戦略
実施期間	2024年11月21日～2024年12月12日
調査対象	業種・規模の異なる複数社（例：売上100億円超～1億円未満など幅広い企業）
回収数	19件

2. 報告内容
②-1アンケート概要と結果

■アンケート結果①：vSphere導入状況（2024年12月時点）



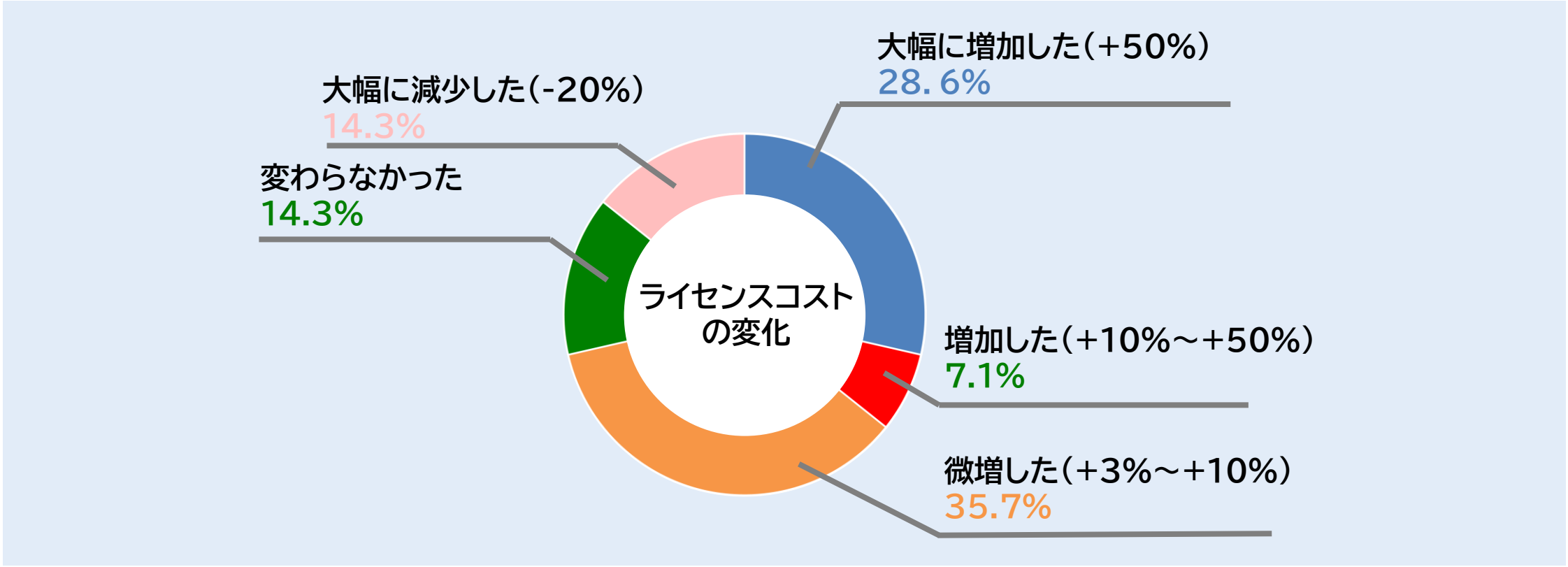
- 回答企業のvSphere導入ステータス
  - 「現在利用している」・・・多数
  - 「過去に利用していたが停止」・・・少数
  - 「導入を検討していない」・・・一部

- ライセンス形態
  - パーペチュアルライセンス（永続）保持 → 約70%
  - サブスクリプションへ移行済 → 約14%
  - 利用停止済み→約7%
  - サービスプロバイダ向けプログラム→約7%

永続ライセンスユーザが多いが、サブスクや他プログラムも散見

2. 報告内容
②-1アンケート概要と結果

■アンケート結果②：23年度と24年度のライセンスコストの変化

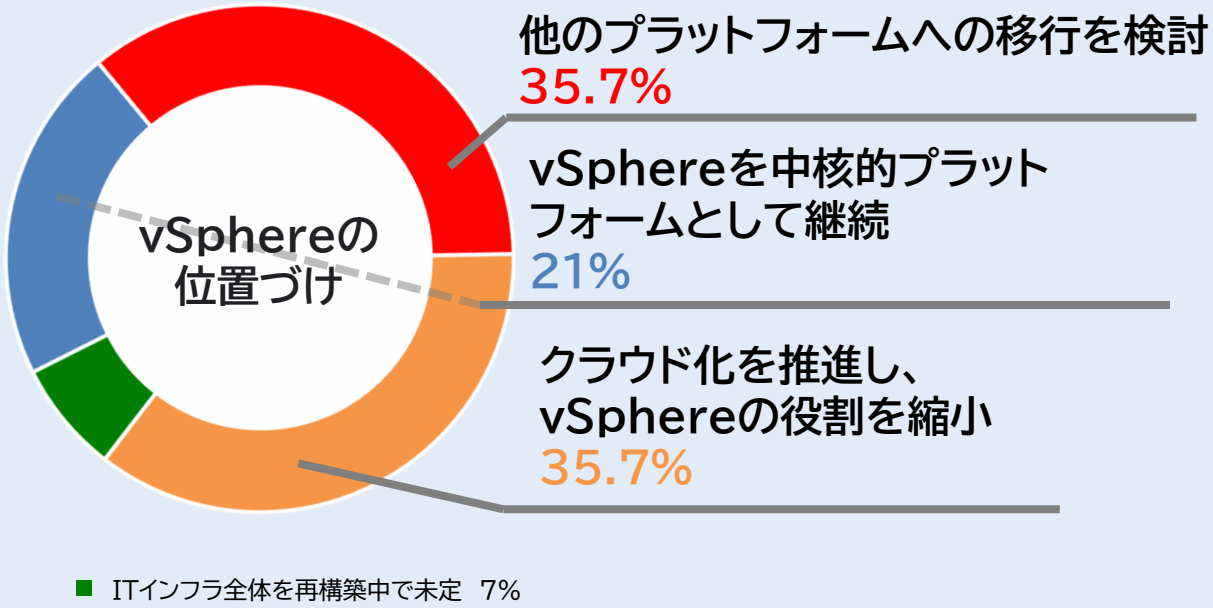


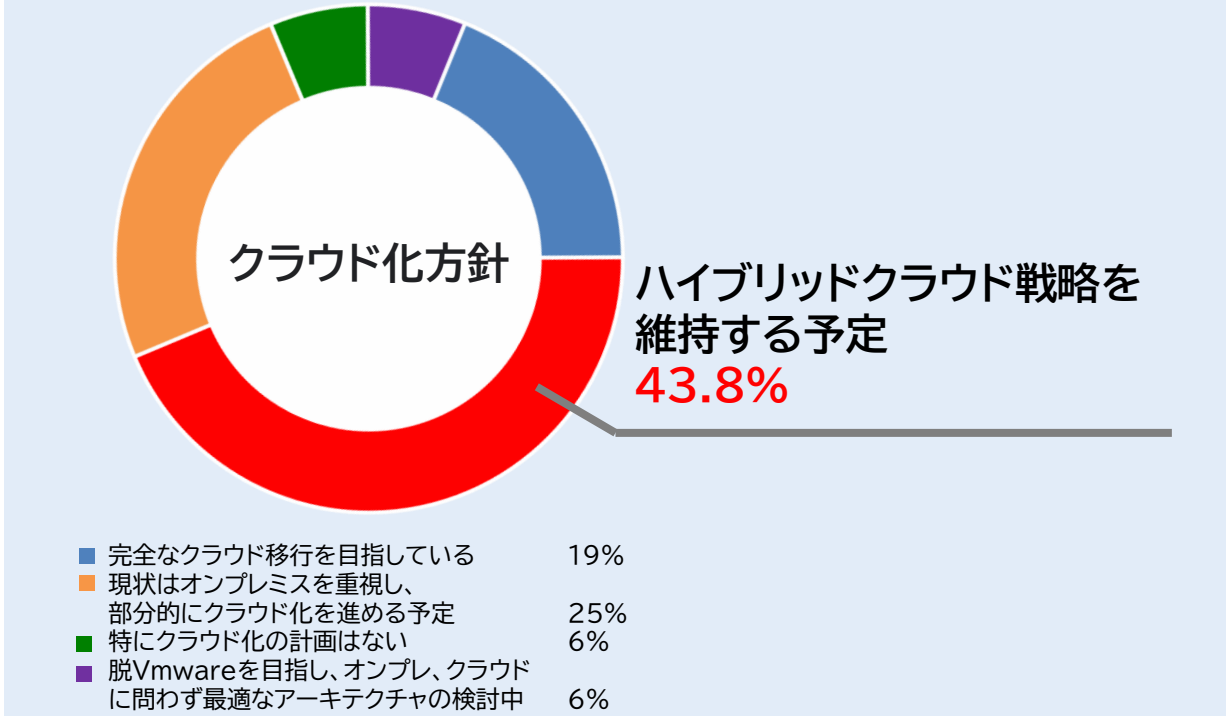
■「コストが増加した」
増加事例：サブスク移行、VCFパッケージへの変更

■「コストが変わらない or 減少した」
減少事例：保守契約打切り、不要サーバ停止、オンプレ縮小

2. 報告内容
②-1アンケート概要と結果

■アンケート結果③：中長期的なITインフラ戦略





- 「クラウド化を推進し、vSphereを縮小」、「完全クラウド移行を目指す企業」が多数
- 「vSphereを中核的プラットフォームとして継続」は2割程度
→コスト交渉もある程度容認

- 「ハイブリッドクラウド戦略を維持」も多数

2. 報告内容
②-2アンケート考察

■23年度と24年度を比較してライセンスコストは変化しましたか？

アンケート結果② - ライセンスコスト変化より

- 「コストが増加した」回答が多数
  - 大幅増（50%以上）:
  - 増加した（+10%以上～+50%未満
  - 微増した（+3%以上～+10%未満）
- 一方で「コストが変わらない or 減少した」例もある
  - 回避策例：保守契約打ち切り、不要サーバー停止、オンプレ縮小

この回答を基準に対象を以下のグループに分類し、考察する

A、コストが増加した企業

・大幅に増加した
・増加した
・微増した

を選択した回答（約70%）

B、コストの影響を受けていない企業

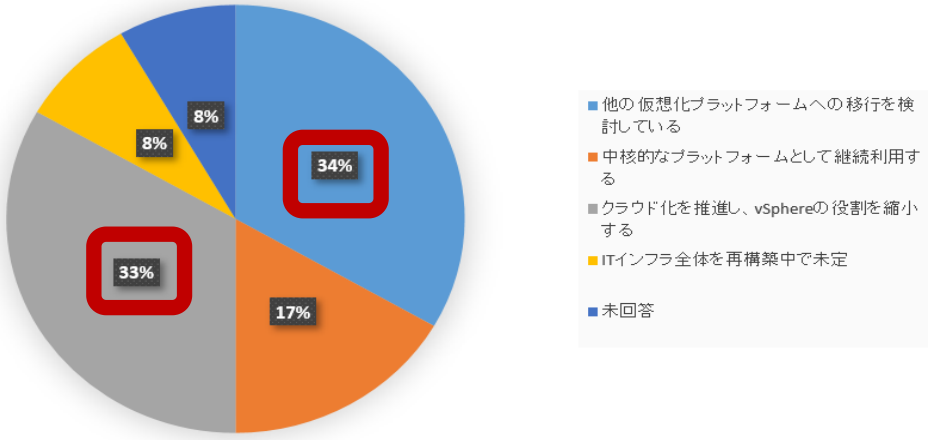
・変わらなかった
・微減した
・減少した
・大幅に減少した

を選択した回答（約30%）

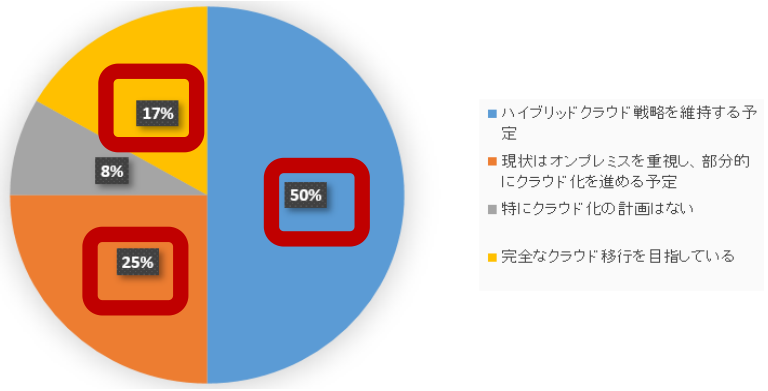
2. 報告内容
②-2アンケート考察 ～グループA～

■グループA(コストが増加した企業)における考察

貴社の中長期的なITインフラ戦略において、vSphereの位置づけはどのように考えていますか？
グループAのみ



中長期的な視点で、貴社のITインフラのクラウド化方針はどのように進めていますか？
グループAのみ



- 多くの回答者がクラウドサービスとの統合でコスト削減を狙っている
- 一方で完全なクラウド化を目指す企業は少なく、8割の回答者が完全にオンプレ環境からは完全には脱却できないと考えている（ハイブリッドクラウド体制）

グループAの多くは、急激なコスト上昇により危機感を持ち、クラウドを活用したコスト低減を狙っている

2. 報告内容
②-2アンケート考察 ～グループA～

■グループA(コストが増加した企業)における考察

■多くの企業がクラウド活用を促進している(会社方針もある)★

■一方で完全な脱VMを掲げている企業は少なかった→完全移行に付随するコストへの懸念★

その他の考察

■保守契約を更新せず活用している企業もある(リスク受容)

■Aグループは、利用サービスとしてVMWareのサービスを多く使っているのではなく、部分的に活用している8割を占めていた
→そのためライセンス改定の影響大

■Aグループにおいて期待するプラットフォームとしてAWSが人気(8割を占めている)★

★ここから予測されるAグループのシステム構成例は、、

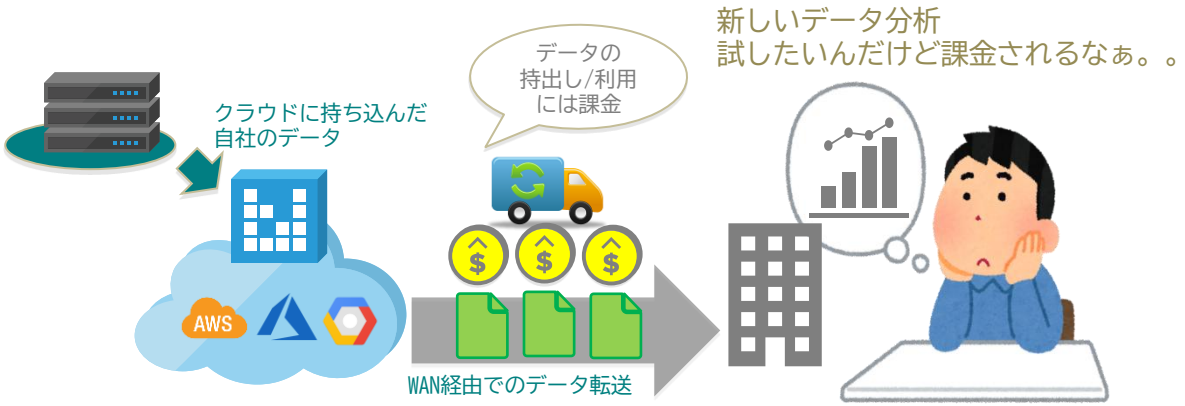
- 強固なセキュリティ対策が必要なマシン、レガシーシステム、クラウドでライセンス取得が難しいマシン ▶ オンプレに配置
- 多くの一般的なマシン ▶ 信頼できる人気なクラウドへ配置

果たしてこれはロックインを回避できているだろうか？

2. 報告内容
②-2アンケート考察 ～グループA～

クラウド移行には、自社のデータがクラウドに「ロックイン」されたり「サイロ化」する問題が潜む

移行先のクラウド以外でのデータ利用に、常に費用が発生し、脱却には多大なスイッチングコスト発生 ≒ クラウドによる「ロックイン」状態



データ転送コストがかかることで、実コスト以外にも

・担当が想定外コストのリスクを恐れてしまう
・クラウドが用意したツールが優先され、アプリがクラウド事業者の仕組みにロックインされてしまう

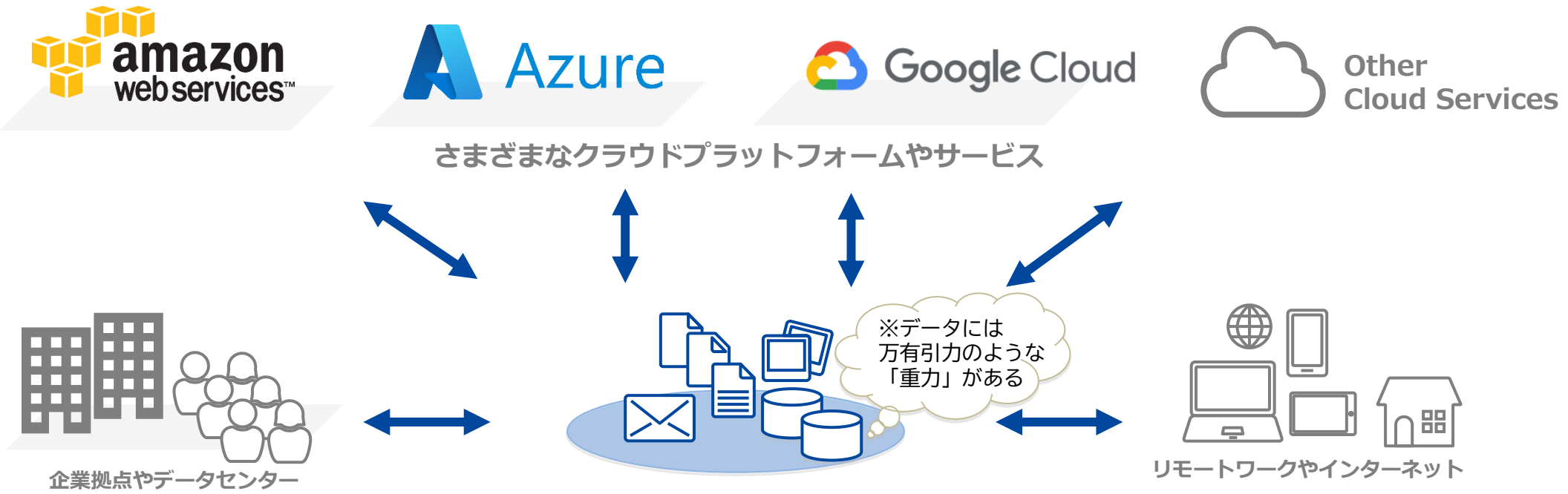
など、オープンなDX活動が阻害されてしまいます

システム毎に最適なクラウド選択した結果、データが「サイロ化」

単にその時最適なクラウドを選んで利用するアプローチだと、一見「マルチクラウド」での利用は進んでも、システムのデータが個々のプラットホームで「サイロ化」し、横断でのデータやアプリの利用にコストがかかってしまう。

2. 報告内容
②-2アンケート考察 ～グループA～

- 大切なのは、**重要な企業価値である「データ」をプラットフォームの中心に置いて考える**こと
  - システムはデータの周囲を取り巻くように作られ、データの周囲で稼働し企業価値を生み出す。（※データの重力）
  - 価値の根源たるデータに、替えはない。**データ「ロックイン」されてしまうことは企業価値を他者に委ねているのと同じ。**
  - ユーザーが**自身のデータ主権をしっかりと握る**ことでこそ、**マルチプラットフォームでの多様な選択肢を実現**できる



データを中心としたプラットフォーム・システムを設計し、企業価値を守るべき

2. 報告内容
②-2アンケート考察 ～グループA～

■グループA(コストが増加した企業)における考察

■クラウド移行後もベンダーロックイン発生リスクはある。
- 例)パブリッククラウド各社の専用サービス依存してしまうケース

■ベンダーロックインを回避する方策の例
- マルチプラットフォーム活用・マルチクラウド活用
- OSS基盤(Kubernetes等)の活用

～適切なロックイン対策案～

× コスト上昇に伴いメインプラットフォームを人気クラウドに変更する

クラウドへ移行した場合でも、単一プラットフォームであれば、ベンダーによってストレージサービスからデータを取り出すコストを引き上げられたら、同じ問題を抱えてしまう(むしろ悪化している、、)

○ 同等の環境をマルチプラットフォームで運用できる体制を整備する

同じシステム構成を作成するもしくは、データを別のプラットフォームに保管し、耐久性を高める

2. 報告内容
②-2アンケート考察 ～グループB～

■グループB(コストの影響を受けていない企業)における考察

パターン1	• グループA(コストが増加した企業)と比べ、台数が少ない回答者(50~100台) なぜなら、VMware利用停止、クラウド移行するといった対策がスムーズにとれるから
パターン2	• すでにクラウド戦略が成功していて、ライセンス改定に先立って、vSphere環境の縮小ができていた
パターン3	• 前述のパターン以外の回答者 • Bグループの中で所持VMが500台以上であり、クラウド活用をしていない回答者 その回答者の回答に着目すると、すでにVMwareの機能を網羅的に活用していた そのためライセンス改定の影響を受けづらかった

B、値上げの影響を受けていない企業
- VM数が100台未満の環境で利用している
- すでにクラウド戦略が成功していた
- VMを多く所有している企業でも、脱ベンダーロックイン状態とは逆にベンダーのサービスを網羅的に利用している場合、利用料改定の影響を回避できた。

2. 報告内容
②-2アンケート考察 ～グループB～

■グループB(コストの影響を受けていない企業)における考察

メリット

■コスト
- 新プラットフォームの切り替えコスト、教育コスト等が不要
- サービス購入時のスケールメリットの享受
- システム統一による運用工数の軽減→結果的なコスト削減
- VMware機能をフル活用が可能で、ライセンス改定の影響を受けにくいことがある

■運用面
- ベンダーとしても大口顧客として手厚いサポートが期待できる
- ベンダーの利用者システム理解や、交渉余地が期待できる

デメリット

■ ライセンス改定や値上げの形式によっては大きな影響を受けうる

■ 他サービスへの移行が困難になる

- 「ベンダーロックインを受け入れる！」という方針で
  ベンダーロックインのメリットが大幅に享受できる可能性がある

2. 報告内容
③まとめ(提言)

まとめ
(提言)

ベンダーロックインによる悪影響を避けるためには・・・

ベンダーロックインを回避する！

- 競合製品を並行利用することでリスク回避
- クラウドもロックインの危険性アリ、ロックインを避けるなら、データを守る体制を作りつつ、マルチプラットフォームも検討要

ベンダーロックインを受け入れる！

- 付随する機能を網羅的に利用しリスク回避
- 他サービスへの移行は困難になってしまう

回避か受け入れるか、どちらかを徹底的に行うことが重要

「とりあえずクラウドにシフト」ではデータを人質に取られ、同じ轍を踏むことになってしまう

- 回避するなら単一点を無くし徹底的に回避すること
- 受け入れるなら使える機能を徹底的に使っていくこと

3. 最後に

活動の感想とコメント	• VMWareへ直接ヒアリングしたいが実現不可であった • 利用規模に対して、想定ほどダメージを受けていない会社もあり面白かった • ほとんどの企業でクラウド移行をしようとしていることがわかった • 各社のインフラ担当者へ自社での今後の検討の参考としていただきたい

2024年度 ITインフラ研究会
分科会B

DXを実現するデジタル技術：AI活用の深化

2025年4月

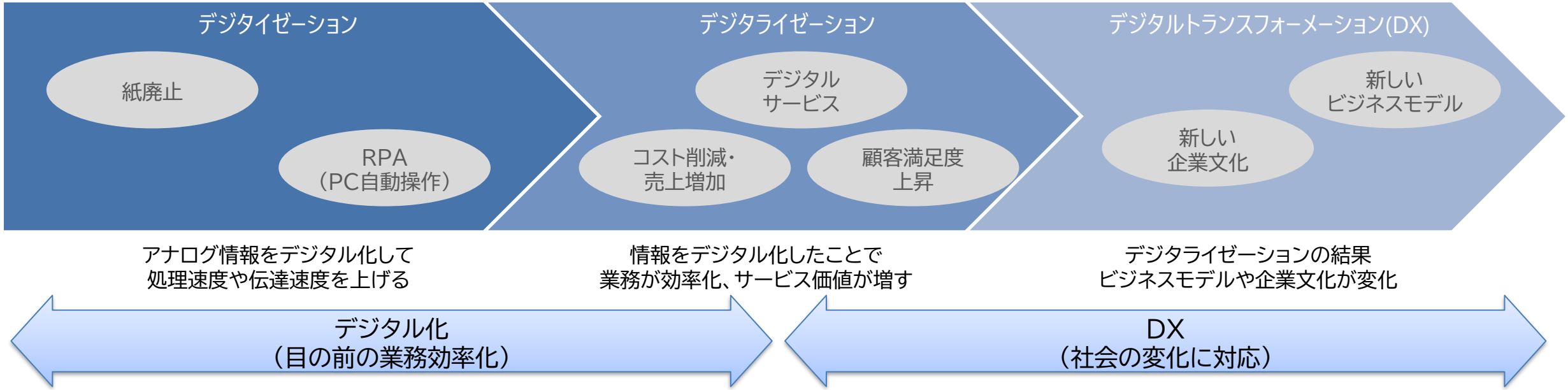
ITインフラ研究会　分科会B

目次

テーマ選定の背景

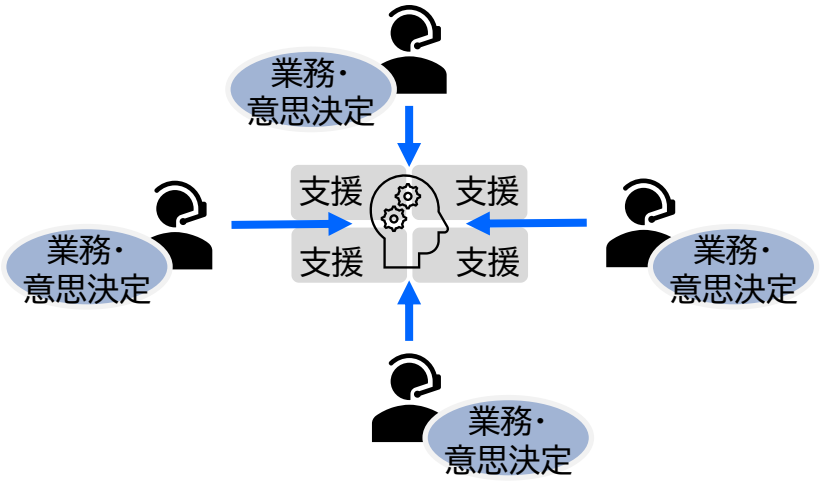
近年、注目を集めている『DX』。
企業や組織は競争力を維持し、さらなる成長を実現するためには、デジタルトランスフォーメーション（DX）を推進する必要がある。
DXは、デジタル技術を活用してビジネスモデルや企業文化などを根本的に変革し競争力を高める取り組みとして注目されているが、
中でもデータの活用や業務の自動化が求められる現代において、AI（人工知能）はその中心的な役割を果たそうとしている。
一方、世間でのAI利用は個人における活用に留まっており、業務における活用が進んでいないと分科会Bは考えている。
分科会Bでは、テーマを『AI活用の深化』とし、AI活用にあたっての課題やその解決の方向性について提言したいと考える。

【デジタルフォーメーション（DX）】の定義】



『AI活用の深化』とは

【現状】
個人利用（**能動的**） ＝ 業務の主体は ”人”

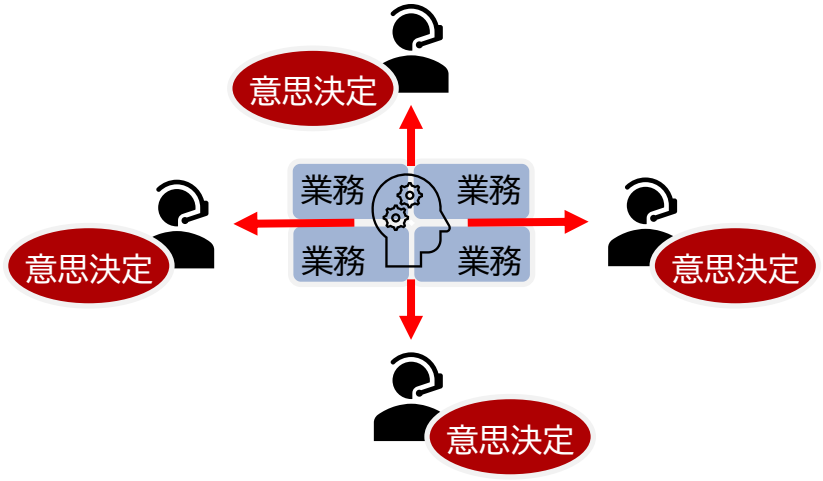


- 業務を行うのは人
- AIは業務の支援ツールとして利用される
- AIを利用する場合は人の指示が必要
- AIが必ずしも業務に組み込まれていない

具体例
- 議事録作成
- 文書作成
- 要約/翻訳　など

深化

【理想】
業務利用（**受動的**） ＝ 業務の主体は ”AI”



- 業務を行うのはAI
- 人はAIが行った業務の結果から意思決定を行う
- 人の指示がなくとも見えないところでAIが利用されている
- AIが業務に組み込まれている、業務を担っている

具体例
- 自動運転
- お客さまへの自動応対
- 商品の提案
- 故障の予測検知
- 配送の自動化

AI活用の現状に対する仮説

分科会Bでは企業におけるAI活用の現状を以下の通りと仮説を立てた。

AIの活用は個人、企業ともに増加している。ただし、資料のベースラインや議事録の作成、要約・翻訳など、AI活用の多くは従来、各個人で実施していた業務の代替（＝個人利用）であり、業務支援ツールとしての利用に留まっている。

即ち、**DXを実現するに至るAI活用**（＝業務利用）ができている企業は少ないと想定した。

また、仮説が正しいとした場合、AI活用が進まない理由は何かに関心を持った。

まずは、利用実態を確認するため、研究会内でAI活用に関するアンケート調査を行った。

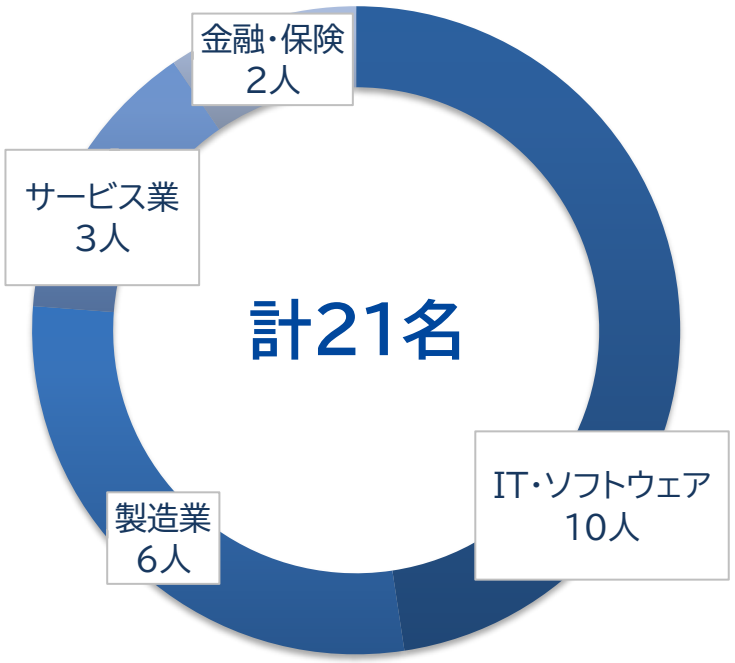
アンケートでは利用実態の他にAI活用の課題についても質問した。次項にアンケート結果を纏める。

AIの業務利用が進まない理由には、以下のような課題が挙げられると想定していた。

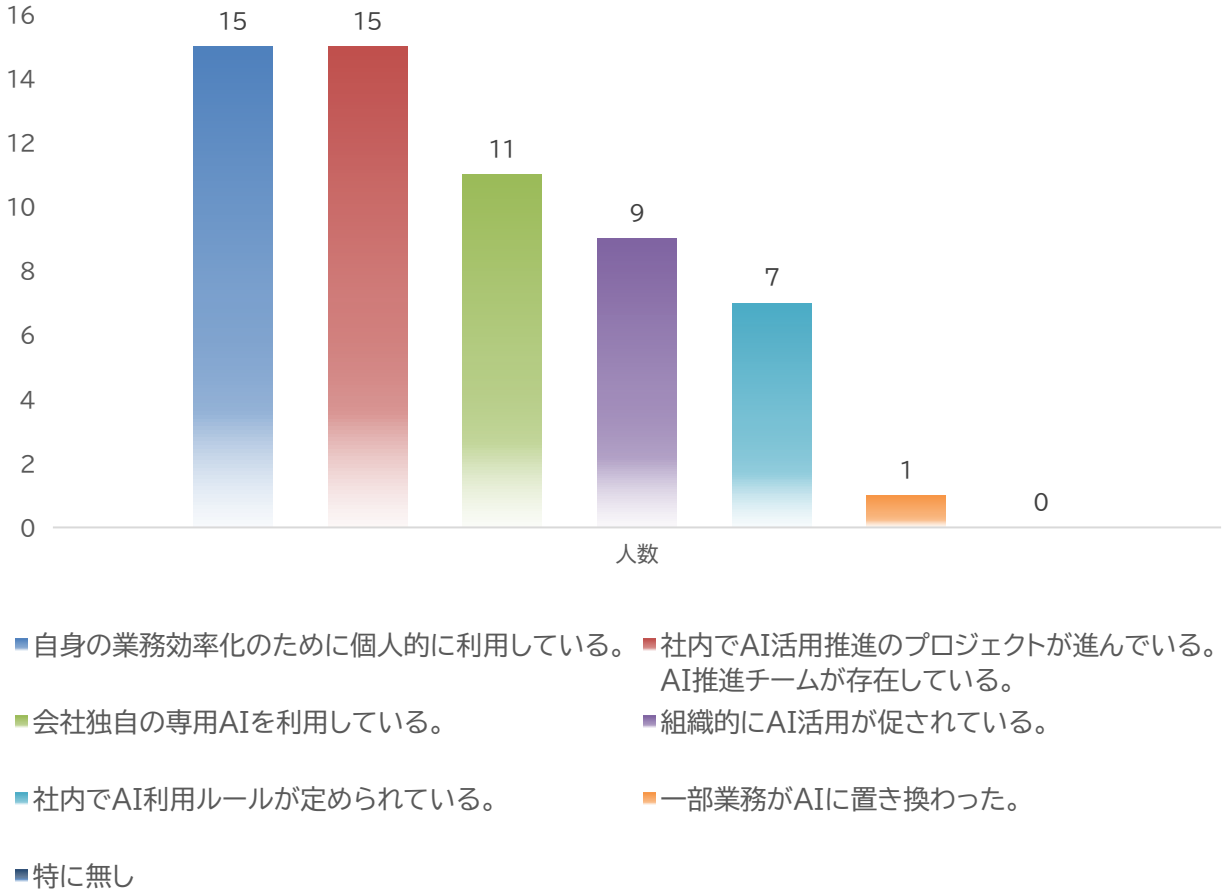
- IT環境、インフラ整備
- 人財不足、スキル不足
- 企業文化、組織体制
- セキュリティ
- コスト、費用対効果
- ガバナンス、法整備　など

アンケート結果

回答者の業種



企業におけるAI活用の実情



アンケート結果

アンケート結果

AI利用に関する満足度

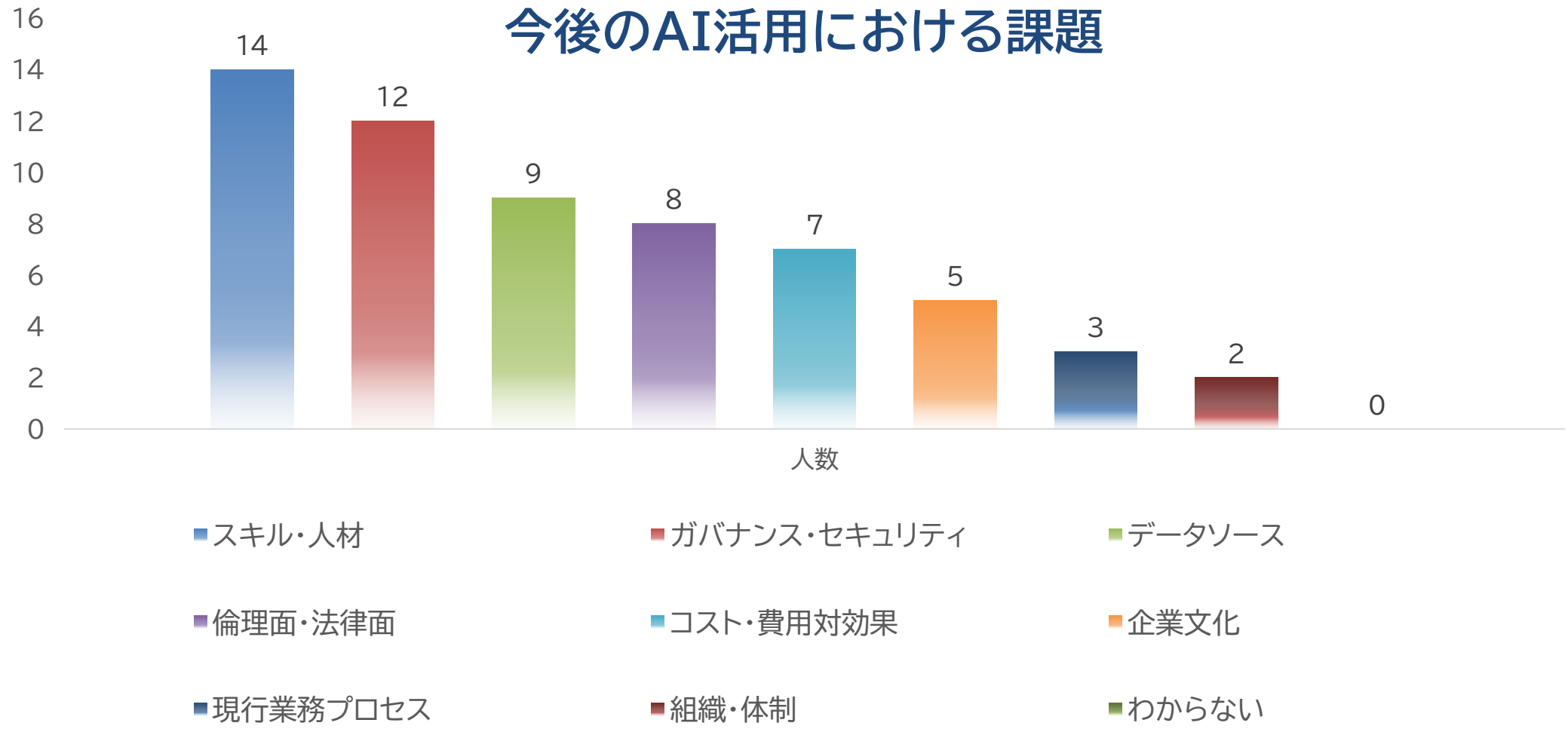
不満点に関するコメント

- 社内情報の検索に対応できていない
- 類推が弱い、ハルシネーションが発生する
- AIの利用アイデアが不足している
- 環境づくりのハードルが高い

AI活用に関する期待

- ドキュメント生成
- SIサービスへの適応
- システム開発・運用への適用
- ノーコード/ローコードの促進
- ヘルプデスク業務における問い合わせ対応
- ルーチンワークの効率化

アンケート結果



アンケート結果の総評

AI活用の現状は概ね仮説通りだった。

AIの推進プロジェクトや推進チームを発足、企業独自の専用AIの構築などAIを活用している企業が多い状況であることは間違いない。

一方でAIの業務利用が進んでいるのは**1企業のみ**に留まった。

分科会Bが想定していた通り、利用用途の多くは文書作成や要約・翻訳、議事録作成など個人利用止まりであると感じた。

AI活用が進んだ先の期待における回答においても業務利用を想定した回答は得られず、個人利用での効率化を期待する回答が占めた。

AI活用に関する不満点として上がった通り、**AI活用アイデアの不足**が否めない結果となった。

AI活用を進める上での課題

今後のAI活用における課題では、「スキル・人材」、「ガバナンス・セキュリティ」に次いで

「データソース」、「ハルシネーション」と技術的な課題が指摘された。

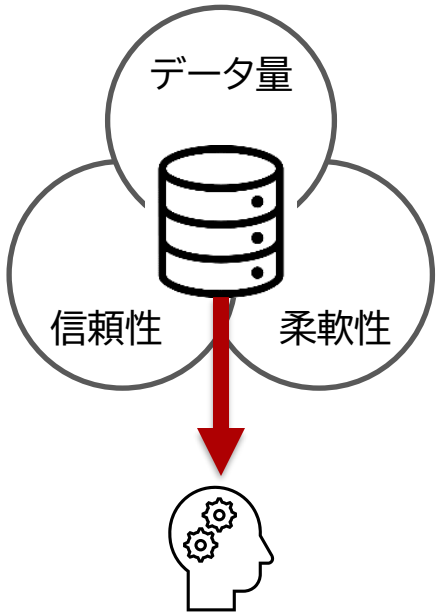
AIが高い精度で判断を行うためには大量かつ質の高いデータによる学習が不可欠となるが、

AIが分析や処理に扱うデータは単に量が多いだけではなく、その信頼性や柔軟性も重要な要素となる。

このため、データ活用の施策を強化し、信頼性の高いデータの収集と管理が求められる。

近年では、リアルタイムデータの需要も高まっている。

AIが即座に分析するためにリアルタイムでのデータ収集と処理能力が、AIの有効活用を支える大きなカギとなる。



そこで、分科会BではAI活用におけるITインフラに着目して、データも含めたインフラ面での課題にフォーカスする。

次項にAI活用におけるインフラ面での頻出課題を纏めた。

ITインフラ面での頻出課題と対応例

課題	内容	対応策の例
計算リソース	大量データをリアルタイムで処理し、学習/意思決定を行うため強力な計算能力が求められる	分散コンピューティング [1] エッジコンピューティング [2]
データソース	自律的に情報を収集/学習/活用するために、大規模でリアルタイムなデータ基盤が必要	リアルタイムデータストリーミング [3] データレイク・データウェアハウス [4]
通信/ネットワーク	クラウド/エッジ間でデータをやり取りするために高速な通信基盤が必要	5G/6G通信 [5]
セキュリティ	悪用や暴走を防ぐための厳格なセキュリティ強化が必要不可欠	フェデレーテッドラーニング [6]

参考文献

[1] HiPro Tech 「分散コンピューティングとは？メリット・デメリットや活用事例を紹介」
https://tech.hipro-job.jp/column/1204

[2] Pro-face 「エッジコンピューティングとは？そのメリットや事例、課題、またクラウドコンピューティングとの違いを分かりやすく解説します」
https://www.proface.com/ja/article/edge-computing

[3] ZOZO 「ZOZOTOWNを支えるリアルタイムデータ連携基盤」
https://techblog.zozo.com/entry/real-time-data-linkage-infrastructure

[4] aws 「ANA グループ 4 万人に展開するデータマネジメント基盤の裏側」
https://aws.amazon.com/jp/blogs/news/ana-data-management/

[5] 総務省 「Beyond 5G（6G）の実現に向けて」
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/nd25760f.html

[6] プライバシーテック研究所 「連合学習はヘルステックと金融で実用が進んでいる？具体的な導入事例をもとに紹介」
https://acompany.tech/privacytechlab/federated-learning-finance-healthcare

結論

アンケートにおいて「スキル・人財」の課題が多く指摘されたが、AI活用を進める上ではAIの知識に長けた人財のみならず、幅広いITインフラの課題を解決できる人財も重要であることを認識した。

AIの活用を深化させるためには、AIを効果的に運用するためのITインフラ環境の整備も求められる。

計算リソースの確保やデータインフラの整備、ネットワークの設計、セキュリティの強化、クラウドコンピューティングなど、ITインフラの対応も不可欠であると考える。

AI活用を深めるためには単にAIそのものの理解にとどまらず、幅広いITインフラの知識・スキルを習得する必要がある。

2024年度 ITインフラ研究会
分科会C

CIS Controlsを用いたセキュリティレベル向上
ケーススタディ

2025年4月

ITインフラ研究会 分科会C

研究テーマ選択の背景/目的

【背景】

- 近年は自社資産としてサーバを設置せず、クラウドサービスを使用する企業が増加している。
- サイバー攻撃が高度化する中、自社のセキュリティを担保するために考慮しなくてはいけないことが、数多くある。

どうすれば安全性を確保できるのか？

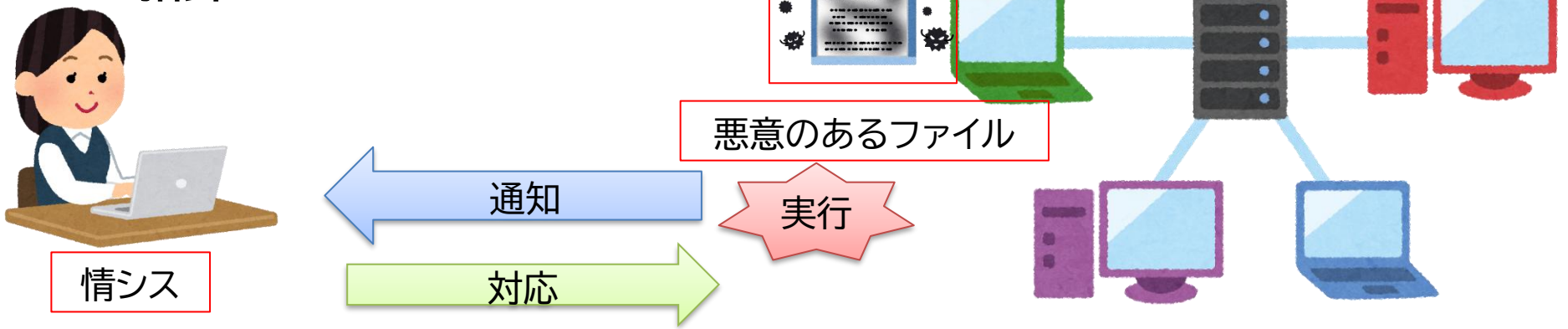
研究テーマ選択の背景/目的

【背景】

- 昨今、新種のマルウェアが1日に100～200万個発見されるといわれている。
  →事前対策では対応しきれない。
- マルウェアに感染してから対応は安全性を確保したとは言えない。
  →ゼロデイ攻撃も含めて、感染を未然に防ぐ必要がある。

- 端末などのエンドポイントを常時監視し、異常や不審な挙動が発生した場合に通知・復旧を支援するEDR(Endpoint Detection and Responce)が重要視されている。

感染や攻撃されてからの通知では遅い。
何か安全性を守るための指針はないか？



研究テーマ選択の背景/目的

【背景】

- NIST(アメリカ国立標準技術研究所)から出ている指針を確認する。
- NISTはスマート電力網や電子健康記録から原子時計、先進のナノ材料、そしてコンピュータチップまで幅広く研究しており、IT業界でもNISTが提供する最新技術、測定技術、技術標準に依存することが多くなってきている。
- NIST CSF(Cybersecurity Framework)、SP800シリーズ等のサイバーセキュリティ対策の国際的かつ代表的なフレームワーク/ガイドラインを発行している。
- 一方、日本ではIPA(情報処理推進機構)が参照するニーズが高いと想定されるNIST文書を翻訳し、解説を公開している。日本政府のサイバーセキュリティ経営ガイドラインでもNISTの規格が参考にされている。

どのガイドラインを参考にするか？

研究テーマ選択の背景/目的

【背景】

- 本分科会では、セキュリティに関する取り組みが先進的であるNISTが作成した**CIS Controls**を取り上げることで、日本における企業のセキュリティレベルの向上の提言ができるのではないか。

CIS ControlsはNISTが作成した他のセキュリティ対策ガイドラインに比べ、具体的な施策が記載。
システム運用担当者やSIerが集まる自チームで取り扱うのに最も適していると考えた

CIS Controlsについて（概要）

- 組織で最低限行うべきサイバー攻撃への対策を提示したガイドライン。
- クラウドサービスやテレワークの増加を受け、2021年にv7からv8へ更新された。

CIS Controlsを用いて、
自己評価から改善手法まで
一貫して実施してみよう！

研究テーマ選択の背景/目的

【目的】

- CIS Controlsによる改善活動がどのようなものか、各社の調査を元にモデルケースを用いて検討し、セキュリティ向上の一助とする。
- 自己評価から改善手法まで一貫して検討することで、実際にCIS Controlsを使用する担当者レベルでの課題を浮き彫りにする。
- メンバーのセキュリティに対する知見を向上する。

CIS Controlsとは？

- CIS Controls（Center for Internet Security Controls）とは、組織内で最低限行うべきサイバー攻撃への対策を提示したガイドライン。
- **自社のセキュリティに漠然とした不安がある方や、何から取り組んでよいのかわからない、といった方々がCIS Controlsを参照することで、セキュリティ対策のポイントを押さえられるようになっている。**

（NRI セキュア ブログより抜粋）

CIS Controlsは、サイバーセキュリティのための一連のベストプラクティスとガイドラインです。これらは、企業や組織がサイバー攻撃から自身を守るための具体的な手順や対策を提供します。
CIS Controlsは、以下のような主要なカテゴリに分かれています：

1.アクセス制御: 不正アクセスを防ぐための対策。
2.データ保護: 機密データの保護と管理。
3.システム監視: サイバー攻撃を検出し、迅速に対応するための監視。
4.インシデント管理: サイバーインシデントが発生した際の対応と復旧。

これらの対策を実施することで、組織はサイバー脅威に対する防御力を強化し、データの機密性、完全性、可用性を保つことができます。

技術的な対策に重点をおいたガイドラインで**あらゆる企業に適応可能**な点が特徴

CIS Controlsとは？

- CIS Controlsのサイバー動向の変化に合わせ、頻繁に更改されており、現在の最新はv8（2021年5月18日リリース）。テレワークの増加やクラウドサービスの活用の増加など環境の変化を受け作成された。
- 18項目の対策分類があり、各要求事項はSafeguards（保護策）として、対策の優先度の指標となるIGs（Implement Groups）を提示する形で整理されている
- 対策分類のうち、「アカウントの管理」、「アクセスコントロールの管理」および「機器やサービスのセキュアな構成や設定」にかかる項目が再整理されており、また、データ保護に関する要求事項が新規で追加されている。

<18項目の対策分類>

< Safeguards（保護策）における優先度 >

CIS Controlsを用いた自己評価について

- 当初、CIS Controlsの要求事項を利用することで、各社のセキュリティ動向の自己評価を実施。結果、セキュリティ対策するべきポイントを提言することを検討した。
- しかし、CIS Controlsの要求事項をそのまま利用することは課題があった
  - 分類が多くあり、アプリケーションに関する項目などITインフラのスコープから外れているものがあった
  - セキュリティの有識者からCIS Controlsを全て実現させることは、日本のITインフラでは現実的ではないという指摘があった

CIS Controlsを質問形式に修正し、各社のセキュリティ動向について調査することを検討

Control N	保護手	保護手段タイトル	質問	資産の種類	セキュリティの機能	IG1	IG2	IG3	回答（Yes, No or N/A）	備考
Control 02 ソフトウェア資産のインベントリと管理	2.1	ソフトウェアのインベントリを作成し維持する	組織の資産にインストールされているすべてのライセンスソフトウェアの詳細なインベントリを作成し維持していますか？また、年に2回またはそれ以上の頻度で見直し更新していますか？	アプリケーション	特定	●	●	●		
	2.2	許可されたソフトウェアが現在サポートされていることを確認する	組織の資産のソフトウェアのインベントリにおいて、現在サポートされているソフトウェアのみが許可されたものとして指定されていることを確認していますか？また、少なくとも毎月またはそれ以上の頻度でソフトウェアリストを見直しソフトウェアのサポート状況を確認していますか？	アプリケーション	特定	●	●	●		
	2.3	許可されていないソフトウェアに対処する	許可されていないソフトウェアが、組織の資産で使用されていないこと、または例外として明文化されていることを確認していますか？また、毎月あるいはそれ以上の頻度で見直しを行なっていますか？	アプリケーション	レスポンス	●	●	●		
	2.4	自動ソフトウェアインベントリツールを活用する	組織全体でソフトウェアインベントリツールを活用し、インストールされたソフトウェアの検出と一覧化を自動化していますか？	アプリケーション	検出		●	●		
	2.5	承認されたソフトウェアの許可リスト	アプリケーションの許可リストなどの技術的な制御を使用して、承認されたソフトウェアのみが実行またはアクセスできるようにしていますか？また、年2回またはそれ以上の頻度で見直しを行っていますか？	アプリケーション	保護		●	●		
	2.6	承認されたライブラリーの許可リスト	技術的な制御を使用して、特定の.dll、.ocx、.soなどの認定されたソフトウェアライブラリーのみがシステムプロセスに読み込みされるようにし、許可されていないライブラリーがシステムプロセスに読み込みされるのをブロックしていますか？また、年に2回またはそれ以上の頻度で見直しを行っていますか？	アプリケーション	保護		●	●		
	2.7	承認されたスクリプトの許可リスト	デジタル署名やバージョン管理などの技術的な制御を使用して、特定の.ps1、.pyなどの許可されたスクリプトやファイルのみが実行できるようにしていますか？また、年に2回またはそれ以上の頻度で見直しを行っていますか？	アプリケーション	保護			●		

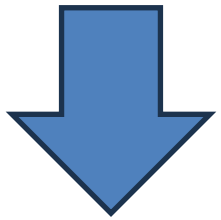
方法：Controlの各項目の回答結果を各社から収集する

・回答基準について
  Yes: 質問の基準を満たしている
  No: 質問の基準を満たしていない
  N/A: 質問の内容が該当しない
（該当しない理由を備考欄に記載）

・アンケートを利用した不明点、課題についても備考欄に記載

自己評価における課題について

■アンケートを作成したが、自己評価をする上で課題が判明
- ■ 対象とするシステムが決められていないため、回答ができない
  - ■ 各社である程度共通的なシステムで評価する必要がある

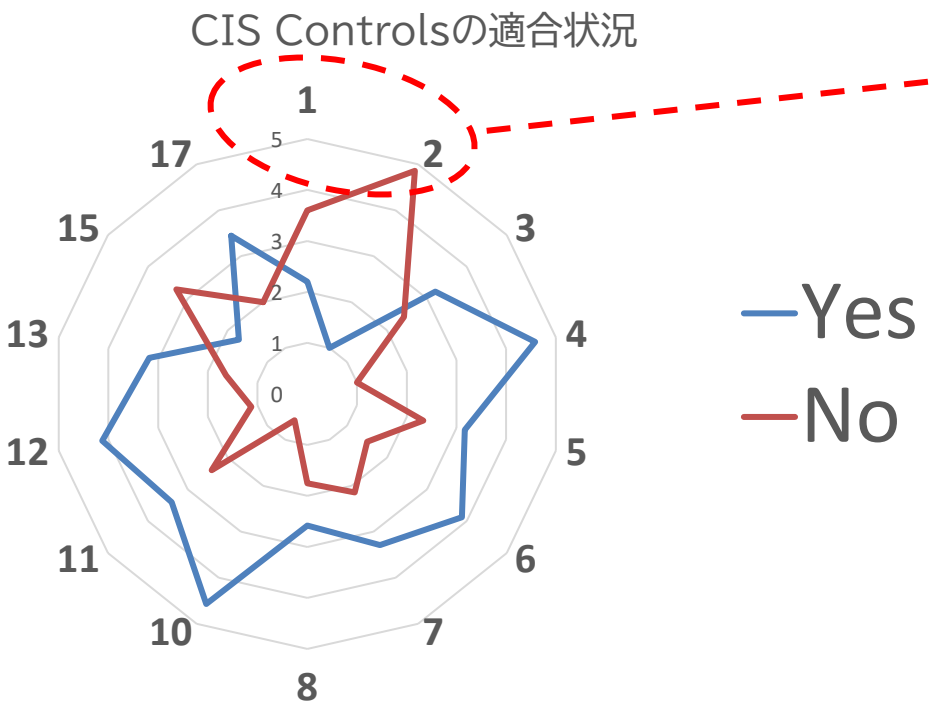


前提条件をしぼるなど工夫をすることで、共通的な評価・回答率向上を期待

＜前提条件＞
- 対象システム：社内OA環境
- 拠点数：1
- その他、CIS Controlsに対するオープンクエスチョンを設定

自己評価結果

- 1,2の項目は各社一貫して低かった
- ここを重点的にとらえ、改善案を練ることとした



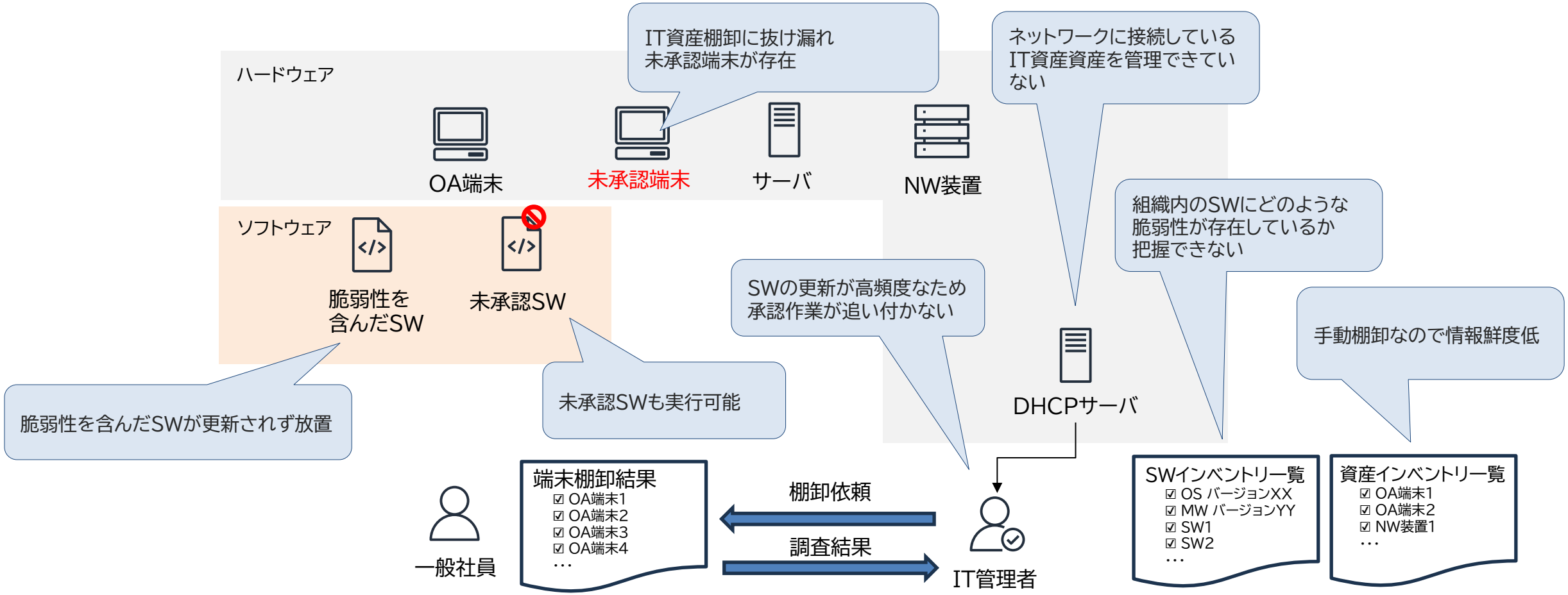
CIS Controls v8（抜粋）

項番	内容
1	**組織の資産とインベントリ管理**
1.3	アクティブな資産ツールを活用する
1.4	DHCPログを利用し組織資産のインベントリを更新する
1.5	パッシブな資産検出ツールを活用する
2	**ソフトウェア資産のインベントリと管理**
2.1	ソフトウェアのインベントリを作成し維持する
2.2	許可されたソフトウェアが現在サポートされていることを確認する
2.3	許可されていないソフトウェアに対処する
2.4	自動ソフトウェアインベントリツールを活用する
2.5	承認されたソフトウェアの許可リスト
2.6	承認されたライブラリーの許可リスト
2.7	承認されたスクリプトの許可リスト

※システム構成ではなく運用に関連する項目は除外

改善案を検討する前提構成

■ モデルケースとして情報資産の管理に課題がある構成を前提とした



改善していくための方法について

■ CIS ControlsのNo.1,2に絞って製品を選定

※比較結果や見解はあくまでも今回の参加メンバーが独自に実施したものであり、JUASの公式見解ではありません。

※〇:機能あり、-:機能なし

製品名 / Control No.	Tanium	PC Matic	Armis	Skysea	iTAssetEye
1.3	〇	〇	-	〇	〇
1.4	〇	-	-	-	-
1.5	〇	-	〇	〇	-
2.1	〇	〇	-	-	〇
2.2	-	〇	-	-	-
2.3	-	〇	〇	〇	〇
2.4	-	〇	-	-	-
2.5	-	〇	〇	〇	-
2.6	-	〇	-	〇	-
2.7	-	〇	-	-	-

改善していくための方法について（スライド14ページの補足）

■改善のための具体的な機能（抜粋）

※括弧内の数字はCIS Controls項目

Tanium

・Tanium discoverにより、非管理端末を検知し、一覧化できる（1.3）
・Tanium assetに拡張モジュールを適用することにより、数十万台のエンドポイント（端末やサーバー）のハードウェアやOSの稼動状況をリアルタイムに可視化し、異常があった場合に即座に報告・対応できる（1.5）

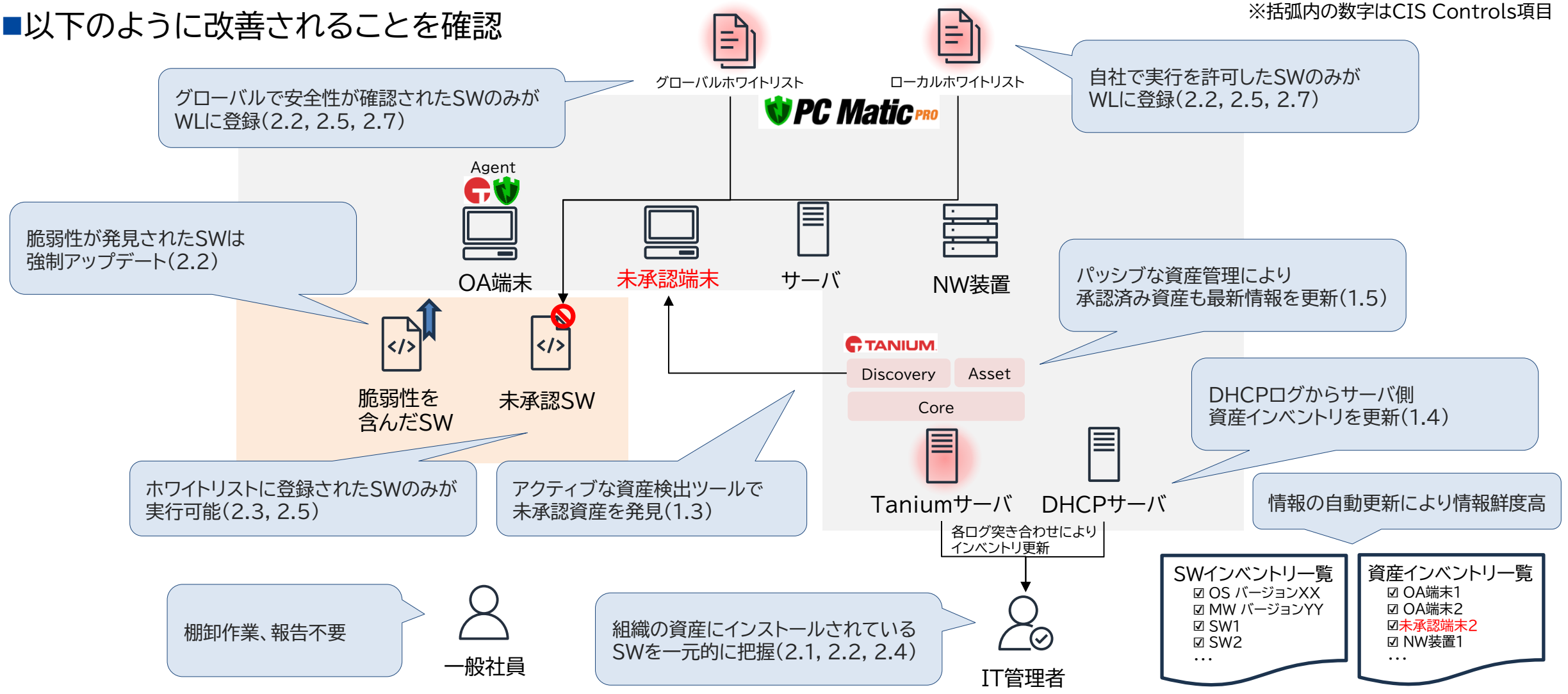
PC Matic

・ソフトウェア資産リストにより、OS にて管理されているアプリケーション一覧を把握することができる（2.1）
・EDRスキャンによって、管理しているアプリケーションの一覧を任意のタイミングで取得できる（2.4）
・アプリケーション・ホワイトリスティング方式によって、脆弱性を抱えているアプリケーションやPC Matic社と自社で許可したアプリケーション以外を実行できない（2.2,2.3,2.5）

改善後のシステム構成と評価について

■以下のように改善されることを確認

※括弧内の数字はCIS Controls項目



取組後の振りかえり

■製品選定の課題
- **情報収集の難しさ**: 日本語の情報が少なく、アクティブなセキュリティ製品を見つけるのが困難。
- **調査レベルの不一致**: 複数の製品評価にあたり、調査対象の基準を揃えるのが難しかった。
- **チェックリストの網羅範囲**: 各セキュリティ製品が独自のサービスを展開しているため、CIS Controlsを満たすかどうかをユーザ側で評価する必要があった。

■アンケートの実施にあたっての課題
- **チェックリストの活用**: 概念的な表現が多く、判断が難しいとのフィードバックを受けた。実際に導入する場合、各社ごとにカスタマイズが必要。
- **モデルケースの設定**: 海外拠点の有無など、導入検討のためのペルソナを決める重要性。

■今後のセキュリティレベル向上の提案
- **CIS Controlsの活用**: 製品選定をCIS Controlsに基づいて行うことで、利用者が判断しやすくなることがわかった。
- **段階的なアプローチ**: アンケートの利用範囲について、事前にステークホルダとの合意形成が重要。

■学びと今後の展望
- **知見の蓄積**: 分科会メンバーは非セキュリティ業務からの参加で、新たな知見を得る機会となった。
- **さらなる研究の必要性**: セキュリティ向上に向けた疑問点を解消するためのさらなる研究と議論が求められる。
- **社内ルールの振り返り**: CIS Controlsを活用に向けて、現在の社内ルールを再確認する良いきっかけとなった。

まとめ

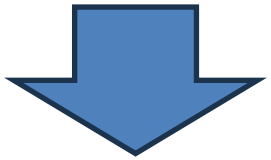
アメリカのセキュリティ導入傾向

システム部門が強く、セキュリティ製品導入など、トップダウンで導入を進められる傾向が強い

日本のセキュリティ導入傾向

ユーザ部門が強く、セキュリティ製品導入など、利用者の利便性と配慮が必要な傾向が強い

CIS Controlsを用いたセキュリティ要件の整理



組織全体でセキュリティに関する意識共有と協力が必要
「セキュリティ」と「利便性」の両立を目指す未来志向の取り組みが重要！

2024年度 ITインフラ研究会
分科会D

ITインフラの適切な維持、管理に向けた運用設計の研究

2025年4月

分科会D

アジェンダ

1. 研究テーマ選定の背景、ゴール
2. 運用設計が重要な理由
3. ITシステムの品質評価指標
4. システム重要度
5. 品質評価指標における運用設計の課題と対策
6. Availability(可用性)
7. Integrity(保全性)
8. Security(安全性)
9. まとめ

1. 研究テーマ選定の背景、ゴール

研究テーマ：ITインフラの適切な維持、管理に向けた運用設計の研究

背景：企業活動においてITシステムは業務効率化や生産性の向上、意思決定の迅速化など企業の成長と持続可能な経営に不可欠な要素になってきている。ITシステムは導入がゴールではなく、安心・安全にシステムを利用・維持することも求められる。我々のチームでは、難易度が上がっている
ITインフラ運用について、導入時の運用設計に着目した。

ゴール：これからのITインフラの維持、管理に向けた運用設計の提言

2. 運用設計が重要な理由

ITシステムは、主に5つのフェーズで異なるタスクや成果物が求められるが、導入フェーズにおける運用設計次第で、ITシステムを安定して稼働させることが困難になる。

ITシステムの安定稼働においては、効率的な運用、障害対応の迅速化、セキュリティの強化、サービス品質の維持などが重要だが、我々のチームでは、ITシステムの品質を評価するための5つの指標を意識して検討を進めた。

3. ITシステムの品質評価指標

本取り組みでは、ITシステムの品質評価するための5つの指標のうち、運用設計において重要なAvailability（可用性）、Integrity（保全性）、Security（安全性）を取り上げる。

指標	
Reliability（信頼性）	システムがどれだけ壊れにくいか、または障害が発生しにくいかを示す。信頼性が高いシステムは、長期間にわたって安定して稼働する。
Availability（可用性）	システムがどれだけの時間稼働しているか、または利用可能であるかを示す。高い可用性は、システムが常に利用可能であることを意味する。
Serviceability（保守性）	システムのメンテナンスや修理がどれだけ容易に行えるかを示す。 保守性が高いシステムは、障害発生時に迅速に修復できるため、ダウンタイムを最小限に抑えられる。
Integrity（保全性）	データが正確で完全であることを保証する指標。保全性が高いシステムは、データの欠損や不整合が発生しにくくなる。
Security（安全性）	システムが外部からの攻撃や内部の不正行為からどれだけ保護されているかを示す。安全性が高いシステムは、データの機密性やシステムの健全性を維持する。

安定したITシステムを提供するには、品質評価指標を意識した運用設計が必要だが、
コストやリソースなど負担を考慮し、一律適用ではなくシステムの重要度に応じた対応も重要。

4. システム重要度

企業や組織では、保有するITシステムがどれだけ重要であるかを示す指標として、システム重要度を設定する。
以下にシステム重要度を決定するうえでの判断基準(例)を記載する。

システム重要度	ビジネスへの影響	事業継続性	ユーザ数	法規制要件	対象システム（例）	備考
High	・ビジネス影響あり（公共サービス、売上や対外取引への影響あり）	・システム復旧1時間以内	・利用者10%以上の影響	あり（資金決済法、個人情報保護法 etc）	・交通システム ・電力xxシステム ・ECサイト ・インフラ基盤（Iaas,基幹NW）	どれか1つでも該当した場合
Middle	・ビジネス影響あり（社内影響）	・システム復旧12時間以内	・利用者10%以下の影響 ・特定ユーザへの影響	なし	・社内システム	複数該当した場合
Low	・ビジネス影響なし	ー	・利用者10%以下の影響 ・特定ユーザへの影響	なし	・開発・テスト環境	

※企業や組織の特性により上記の重要度判定の基準は変わりますので、参考情報としてご利用ください。

5. 品質評価指標における運用設計の課題と対策(1)

5つ品質評価指標のうち、運用設計時に特に検討が重要だと考えるAvailability(可用性)、Integrity(保全性)、Security(安全性)について、それぞれのあるべき姿と課題と対策を整理した。

Availability(可用性)を確保するためにも「監視」は重要な運用設計のポイントと考える。

あるべき姿	システム重要度に応じた、監視項目や取得頻度、閾値が明確に設けられており、変化の発生や予兆を検知すること。 問題を早期に発見して対応できるようにすること。
具体的課題	・監視の改善がプロセスに組み込まれていない ・システムの増加に伴い、監視運用への負荷も増加 ・アラート検知が多発するなど、要不要の精査が必要 ・監視対象の状態は収集しているが、分析し生かしきれていない
対策	・効率を上げるためにツールを適用することを設計時点で組み込んでおく ・システムの重要度ごとに収集する項目、取得頻度、検知する閾値、アラートへの対応を基準化 ・性能データの収集、検知を自動化 ・機械学習等を利用し、変動しきい値を導入。アラートの精度を向上 ・機械学習等を利用し収集したデータを分析。平時と比較した異変に対しアラートを出す

※ここでは、運用・保守フェーズでの設計を意識しているため、システムの冗長化や災害対策等の考慮は除く

5. 品質評価指標における運用設計の課題と対策(2)

Integrity(保全性)を確保するためにも「バックアップ・リストア」は重要な運用設計のポイントと考える

あるべき姿	管理対象のITインフラのシステム重要度に応じたバックアップの頻度や保存の基準、システム復旧の基準が明確に設けられており、それらが適切に実施されていること。
具体的課題	・障害発生時の迅速な復旧 ・統一されておらず、方法や運用がバラバラ ・システムの増加に伴い、運用及びストレージのコスト増大化 ・障害発生時の迅速な復旧 ・実際の障害時にリストアできる人員がいない ・リストアの依頼が多く運用者に負担がかかっている(ファイルサーバ)
対策	・運用視点での工夫、日々の運用におけるルールを設計時点で組み込む ・システムの重要度を区分化 ・重要度ごとに頻度や保存期間、システム復旧までの期間を基準化 ・日々のバックアップ運用及び障害時のリストア自動化 ・普段からバックアップ、リストア環境教育を行い、環境への知識を養う ・ユーザに復元権限付与する

5. 品質評価指標における運用設計の課題と対策(3)

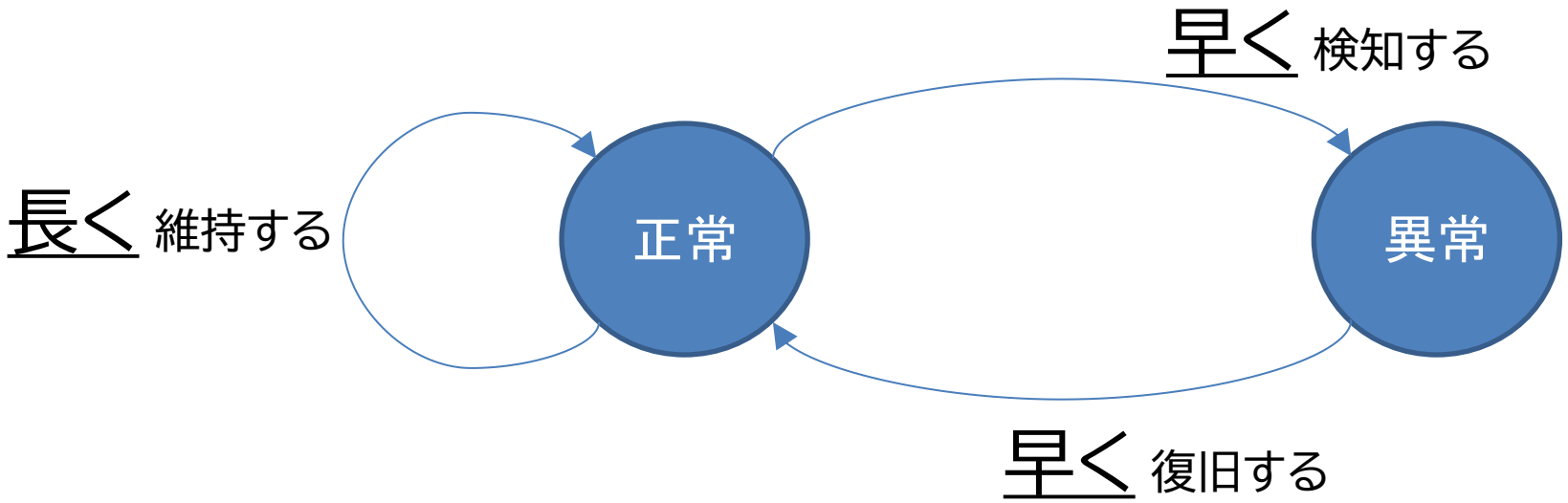
ITシステムを安心・安全に提供するには**Security(安全性)**の「**脆弱性対応**」は重要な設計のポイントと考える

あるべき姿	管理対象のITインフラの脅威や守りたい資産に対して、適切にリスクを評価する基準やセキュリティ対策の基準が明確に設けられており、それらが守られていること
具体的課題	・適切な脆弱性の対応がとれていない ・必要性に応じたアカウント権限の管理ができていない ・ソフトウェアのライフサイクル ・保守切れしたHW/SWの運用
対策	・脆弱性対応の計画(情報取集・暫定恒久対応) ・立場に応じたアカウント権限の付与 ・数年先を見据えた保守切れ対応・システム改修の計画

6. Availability(可用性) 監視対応方針

Availability(可用性)が高いシステムとは“稼働率が高い(利用したいときに利用できる)”システムであり、一般的には冗長構成を組むことなどが最もイメージしやすい設計ポイントとなる。
ただ、可用性を下記のように定義すると、システムの状態を適切に把握すること(監視運用)も可用性向上に重要な要素であることが分かる。

- 異常状態をいかに早く検知し、いかに早く復旧するか
- 正常状態をいかに長く維持するか



6. Availability(可用性) 監視設計項目

“監視運用”として求められる一般的な設計項目を以下に整理する。

項目	内容
ネットワーク監視設計	・ネットワーク疎通(Ping) ・通信量
サーバ監視設計	・サーバリソース(CPU、メモリ、ディスク容量) ・従量課金状況
アプリケーション監視設計	・ポート死活(HTTP,HTTPS,SMTPなど) ・ポート応答時間
DB監視設計	・DB容量 ・DB接続数
ログ監視設計	・OSログ,APログ,DBログ
アラート・通知設計	・閾値を設定し、検知 ・メール等、通知を行う。

- チームで監視に関する設計項目を洗い出したが、それぞれの会社での設計項目に大きな遜色はなく、どの会社もある程度は一般的に提唱されている設計項目は充足していることが分かった。

6. Availability（可用性） 具体的課題とその分類

一般的な監視項目は設計の中で取り込んでいるが、実運用においては様々な課題があることが確認できた。
その中で、共通的に課題として認識されていたもの大別すると以下の2つに集約することが出来た。

課題1 人手での対応が追い付いていない

課題2 監視の改善がプロセスに組み込まれていない

■**チーム内アンケートで見えた課題**

① 監視運用の負荷が増加傾向にある

② アラート検知が多発するなど、要不要の精査に時間を要している

③ 監視対象の状態は収集しているが、分析・活用されていない

④ 設計当時から監視運用のプロセスが変わっていない

⑤ 基準が統一されていない部分もあり、システムごとに運用がバラバラ

⑥ 基準が統一されている部分においては、監視運用を変更しづらい

人手での対応が
追い付いていない

改善活動が監視プロセスに
組み込まれていない

6. Availability(可用性) 監視課題(1)

課題1 人手での対応が追い付いていない

<課題発生の背景の考察>

✅ 近年、システムを取り巻く環境は複雑化※ しており、
旧来の監視機能だけでは効率的・効果的に監視運用を行うのが難しくなってきている。

※ 例：メインフレームに集約されていたシステムが、様々なミドルウェアが導入された役割別のサーバに分散
オンプレやクラウドなど複数環境での運用

<運用設計段階で考慮すべきこと>

効率を上げるためにツールを適用することを設計時点で組み込んでおく。

◇監視負荷増大のポイントを考察の上、ツール導入により改善を図りたい部分を見極める。

【ツール適用検討観点(例)】
- 情報量が従来のシステムと比べ膨大傾向に無いか
- 情報が散在していないか
- 収集した情報の視認性は高いか
- 検知・通知に自動化の余地はないか
- 復旧作業に自動化の余地はないか

**システムが複雑化・肥大化していく中で
情報の取集、分析、可視化、検知、対応といった一連の
プロセスのどの部分に改善ポイントが出るかの見極め**

6. Availability(可用性) 監視課題(2)

課題2 監視の改善がプロセスに組み込まれていない

<課題発生の背景の考察>

✅ 運用・保守フェーズに入ると、個別の発生事象とその対策についての議論に終始し、
全体横断での改善検討に話を展開することが難しい。

✅ 監視における設計は全社基準を作成してそれに準拠する方法が一般的であるが
統一的な管理が出来るメリットがある一方で、全社基準のため改変していくのが難しいという側面がある。
(監視に限らず、非機能系は一度定めた要件は変更しづらい傾向がある。)

<運用設計段階で考慮すべきこと>

監視改善活動を運用項目(運用プロセス)の一つとして設計時点で組み込んでおく。

◇運用・保守フェーズに入ってからの情報をInputに見直しを行うことを設計時点で定義し、実践する。

【改善検討観点(例)】
- 予兆検知などを組み込み、監視の在り方の抜本的な見直し(プロアクティブな対応を検討)。
- 監視設計項目(前述)の設定値の見直し(運用フェーズを加味して適した閾値の再設定など)
- 検知イベントの削減(不要なイベントの見極めと削除など)
- 自動化検討(同一作業の機械化など)

6. Availability(可用性) 監視設計の提言

Availability(可用性)を高めるという視点においては
冗長化、オートスケール、BCP対策といったような観点に目が向くケースが多いが
システムの安定稼働においては監視運用も重要な要素であることを認識するべきである。

近年のオブザーバビリティやAIOpsなどをキーワードにした技術・製品の進展は大きいため、
効率を上げるためにツールを活用すること意識して最新の動向などの情報収集、及び、適用検討を
早い段階で進めていくことが重要と言える。

どの会社でも監視のプロセスや基準が存在するとは思うが
定期的に現状の監視運用の改善ポイントを定め、改善を図っていくことが必要。

6. Availability(可用性) ツール(1)

ツール名	ツール特性
Splunk Splunk (スプランク) | 企業のレジリエンス強化の鍵となる	データの収集、検索、監視、分析を行うためのツール リアルタイム分析やアラート機能、ダッシュボードや機械学習を用いた予兆検知が可能
Kompira 運用自動化プラットフォーム Kompira	システム運用の効率化と自動化を支援するためのツール アラートの判断やエスカレーション電話の自動化が可能
Dynatrace Dynatrace (ダイナトレース) | 最新のクラウドの正しい運用法	ITサービス運用と保守の課題を解決するための強力なオブザーバビリティとAIOpsプラットフォーム サーバにエージェントを実装することでシステム全体の包括管理が可能
ServiceNow ServiceNow - AI を、あなたの役に立つものへ。	運用効率を向上させるための包括的なクラウドベースのプラットフォーム ITサービス管理やIT運用管理、カスタマーサービス管理などが可能
DATADOG クラウド時代のサーバー監視&分析サービス | Datadog	クラウドベースのモニタリングおよびセキュリティプラットフォームで、インフラストラクチャ、アプリケーション、ログなどを統合的に監視するための多機能なツール
PagerDuty PagerDuty | インシデント管理プラットフォーム | PagerDuty株式会社	インシデント管理と運用の効率化を支援するための強力なプラットフォーム リアルタイムインシデント管理やAIOps、オンコール管理が可能
New Relic New Relic | Monitor, Debug and Improve Your Entire Stack	アプリケーションパフォーマンス管理とオブザーバビリティを提供する強力なプラットフォーム フルスタックオブザーバビリティやリアルタイムモニタリング、ダッシュボードなどが可能

7. Integrity（保全性） バックアップ・リストア対応方針

Integrity（保全性）を高めるためには、管理対象システムの有事の際に、迅速にシステムを復旧させるためのデータ保護や復旧させるための手順の確立、日々の備えが設計のポイントとなる。
また、システムの重要度に応じて適切な対策を設計することはコスト効率の観点でも重要である。

以下の5つの要素を踏まえて運用設計をする。

1. **データの保護:** データ損失はビジネスに重大な影響を与える可能性がある。バックアップ運用設計により、データが安全に保管され、必要な時に復元できるようになる。
2. **迅速な復旧:** システム障害やデータ損失が発生した場合、迅速に復旧できることが重要。適切なバックアップ設計により、ダウンタイムを最小限に抑え、業務の継続性を確保する。
3. **コスト効率:** バックアップ運用設計により、必要なリソースを最適化し、コストを削減できる。例えば、適切なバックアップ頻度や保存期間を設定することで、ストレージコストを管理できる。
4. **コンプライアンス:** 多くの業界では、データ保護に関する規制が存在する。バックアップ運用設計により、これらの規制を遵守し、法的リスクを回避できる。
5. **リスク管理:** 自然災害やサイバー攻撃などのリスクに対して、データのバックアップは重要な防御手段となる。運用設計により、リスクを評価し、適切な対策を講じることができる。

7. Integrity（保全性） リストアのレベル定義

バックアップ・リストア運用設計において、以下の影響判定項目の評点に基づき、重要度レベルを決定し、
レベルごとのRTO（システム回復時間）、RPO（システム回復ポイント）を定義し、基準を検討する方法もある。

影響判定項目	評点		
社外影響	あり：10	なし：0	-
社内業務影響	あり：5	なし：0	-
重要法令影響	あり：3	なし：0	-
即時影響有無	即時：5	猶予あり：3	なし：0
システム停止許容時間	1時間以内：0	当日中：-3	翌日以降可：-5

スコア算定

スコア	重要度レベル	RTO（システム回復時間）	RPO（システム回復ポイント）
15以上	High	1時間以内	30分以内
5以上、15未満	Middle	数時間から1日以内	数分から数時間以内以内
5未満	Low	数日以内	1日以内

7. Integrity(保全性) 設計案(1)

バックアップ・リストアの運用設計にあたり、以下項目の考慮ポイント、設計指針を考慮する。

項目	考慮ポイント	設計指針	備考
取得頻度	データの更新頻度にて取得頻度を定義	• データの更新が頻繁な場合: リアルタイムまたは数分から数十分ごとバックアップ取得 • データの更新頻度がやや低い場合: 日次バックアップ • データの更新が比較的少ない場合: 週次バックアップ • データの更新がほぼ発生しない場合: システム変更時バックアップ	
保存期間	業務要件、コンプライアンス(法的規制)、また取得したバックアップデータの種類から保存期間を定義	• 短期保存:30日 リアルタイムのバックアップデータ、毎時バックアップデータ • 中期保存:3か月 日次バックアップデータ、週次バックアップデータ • 長期保存:5~7年 月次バックアップデータ、年次バックアップデータ	

7. Integrity(保全性) 設計案(2)

項目	考慮ポイント	設計指針	備考
保存世代	データの重要度や変更頻度、ストレージ容量、法的要件にて保存世代を定義 ただし、ストレージ容量とコストのバランスを考慮する	• データの更新が頻繁な場合: フルバックアップ:毎日24世代を保持し、1週間分(168世代)を保持(1日の間に発生したすべての変更をカバー)。週次で7日前の世代を削除。 10分ごとの増分or差分バックアップ毎日144世代を保持(フルバックアップ以降のすべての変更)。1週間分(1008世代)を保持する場合、週次で1日分の古い世代を削除。 • データの更新頻度がやや低い場合: 毎週フルバックアップを取得し、過去4週間分(4世代)を保持(1ヶ月以内のデータを確実に保護)。週次で5週前の世代を削除。 日次増分or差分バックアップを過去14日分(14世代)を保持(直近2週間のデータの変更をすべてカバー)。日時で15日 • データの更新が比較的少ない場合: 毎月フルバックアップを取得し、過去3ヶ月分を保持(中期的なデータ保護が可能)。月次にて4ヶ月前の世代を削除。 週次増分or差分バックアップを取得し。過去8週間分を保持(2ヶ月以内のデータの変更をすべてカバー)。 • データの更新がほぼ発生しない場合: システム変更やアップデートの前後にフルバックアップを取得し、3世代分を保持。(システム変更前の状態に迅速に復元することが可能)	

7. Integrity（保全性） 設計案（3）

項目	考慮ポイント	設計指針	備考
取得方法	業務要件、コンプライアンス（法的規制）、また取得したバックアップデータ種類、求められるRTO、RPOにより取得方法、取得間隔を定義	• データの更新が頻繁、高可用性システム、法的・規制、高価値データの場合: フルバックアップ1回/時間、増分or差分10分/回 • データの更新頻度がやや低い場合: フルバックアップ1回/週、増分or差分1回/日 • データの更新が比較的少ない場合: フルバックアップ1回/月、増分or差分1回/週 • データの更新がほぼ発生しない場合: フルバックアップ1回/システム変更時	バックアップ取得時間短縮のため、スナップショットバックアップによるバックアップ、また、スナップショットからの合成フルバックアップを考慮する
保存場所	データの安全性、アクセスの容易さ、コスト効率などを考慮して保管場所を定義	• 3つ データコピーを保持（オリジナルと2つのバックアップ） • 2つの異なるメディアでデータの保持（オンサイトストレージとクラウドストレージ） • 1つのオフサイトにオフサイトコピーを保管	
暗号化	バックアップデータの暗号化は、不正アクセスからのデータ保護、機密情報や個人情報が漏洩するリスク低減、改ざんや破損に対するデータ耐性および整合性の保護が必要ある場合考慮する	• バックアップデータを取得時に強力な暗号化アルゴリズムを使用して暗号化を実施 • 号化キーは安全に管理し、アクセス制御を行う	オンプレミス：バックアップソフトウェアを使用して、バックアップデータを暗号化 クラウドサービス：クラウドプロバイダーが提供する暗号化機能を使用

7. Integrity（保全性） バックアップ種類（1）

バックアップはシステム全体の保護を目的としたシステムバックアップとシステム内データの保護を目的としたバックアップがある。

区分	システムバックアップ	データバックアップ
対象	• OS • システム設定 • インストール済みのアプリケーション • ドライバ など	• ドキュメント（Word, Excel など） • 写真や動画 • 音楽ファイル • 重要な業務データ など
目的	• システム全体をバックアップし、OSがクラッシュした場合やハードウェア障害時に、元の状態に復元できるようにする。 • （例：Windowsの「システムイメージの作成」、Macの「Time Machine」など）	• 誤操作やデータ破損、ウイルス感染などに備え、個別のファイルやフォルダをバックアップし、必要なデータを復元する。
特徴	• OSが含まれるため、完全復旧が可能（新しいPCやHDDにそのまま復元できる） • 容量が大きくなりがち • 一般的に定期的なフルバックアップが推奨される	• ファイル単位で復元可能（OSやアプリは含まれない） • 変更があったファイルだけをバックアップする増分・差分バックアップが可能で、ストレージの節約になる
用途	• OSや環境をそのまま復元したい場合（PCの完全復旧用）	• 重要なファイルを守りたい場合（仕事や個人データの保護）

7. Integrity（保全性） バックアップ種類（2）

コスト効率を意識したバックアップ設計において、適切な種類のバックアップ手法を採用する。

	フルバックアップ	差分バックアップ	増分バックアップ	ミラーリング
概要	すべてのデータをバックアップ	最後のフルバックアップから変更されたデータのみをバックアップ	前回のバックアップ（フルまたは増分）以降に変更されたデータのみをバックアップ	バックアップ対象の最新データだけをリアルタイムまたは定期的にコピー
メリット	• 完全なバックアップが取れるため、単体で復元が可能 • 復元が簡単（1回のリストアで完了）	• フルバックアップより容量が小さく、時間も短縮できる • 復元時にはフルバックアップ＋最新の差分バックアップだけでOK（簡単）	• 最も容量を節約できる • バックアップ時間が短い	• 即座に復元可能（コピーするだけ） • データが常に最新状態に維持される
デメリット	• 時間と容量を多く消費する（データ量が多いと負担大） • 頻繁に取るのは非効率	• 差分データが増えると、フルバックアップとの差が大きくなり、容量・時間が増加 • 頻繁に差分を取ると、フルバックアップの頻度を上げる必要あり	• 復元が複雑（フルバックアップ＋すべての増分バックアップが必要） • 1つでも増分バックアップが欠損すると、復元できない可能性がある	• 誤削除やウイルス感染が即座に反映される（巻き戻しができない） • 過去の履歴を保持できない
使用例	• システムや重要データの初回バックアップ • 定期的に（例：週1回）取得し、差分・増分バックアップと組み合わせて運用	• 日次バックアップ（週1回フルバックアップ＋毎日差分バックアップ） • システム復旧を考慮したデータ保護	• クラウドバックアップ（容量節約のため） • データの頻繁な変更がある環境（1日数回の自動バックアップ）	• RAID構成（ミラーリングでHDD障害対策） • 業務システムのリアルタイムバックアップ

7. Integrity（保全性） 具体的課題とその分類

一般的なバックアップ項目は設計の中で取り込んでいるが、実際の運用においては様々な課題があることが確認できた。その中で、共通的に課題として認識されていたもの大別すると以下の2つに集約することが出来たが、本取り組みにおいては、運用設計で重要となる課題1に着目した。

課題1 障害発生時の迅速な復旧

課題2 バックアップ環境の最適化

■チーム内アンケートで見えた課題

① 迅速な復旧が可能な仕組みが提供できていない

② 実効性のあるシステム復旧のテストや訓練ができていない

③ 基準が統一されておらず、運用が曖昧になっている

④ データ容量増加により迅速なシステム復旧が難しくなっている

⑤ ランサムウェアによるバックアップデータの改ざんリスク

⑥ 複数バックアップ環境の利用や取得環境の複雑化により管理が煩雑になっている

⑦ データ容量の増加によりコストが増加している

障害発生時の迅速な復旧

バックアップ環境の最適化

7. Integrity（保全性） バックアップ・リストアの課題

課題1　障害発生時の迅速な復旧

＜課題発生の背景の考察＞

✅ 企業活動においてITシステムは業務効率化や生産性の向上、意思決定の迅速化など企業の成長と持続可能な経営に不可欠な要素になっており、システム保全における要求事項も高まっている。
また、ITシステムの技術革新により、導入されるシステムは複雑化し、データの肥大化している。
これらにより、技術力の向上やサポート範囲の拡大が求められ運用・保守要員の負荷は拡大傾向にある。

＜運用設計段階で考慮すべきこと＞

迅速にシステムを復旧させるため、運用視点での工夫、日々の運用におけるルールを設計時点で組み込んでおく。
◇運用・保守フェーズにおいて有事の際の対応に向けた取り組みを設計時点で定義し、実践する。

【システム復旧時間の短縮化の検討観点（例）】
- データリストア時間を短縮するための仕組みは考慮したか
- 障害発生を想定したテストは組み込めたか
- 定期的な復旧訓練の計画は立てたか
- 有事の際のルールや基準は明確になっているか
- 復旧手順の簡素化のための自動化は検討したか
- 復旧手順書、チェックシートは用意したか

**システムが複雑化・肥大化していく中で
どのようにしたら有事の際の対応が
円滑かつ迅速にできるのかの見極め**

7. Integrity（保全性） バックアップ・リストア運用の提言

Integrity（保全性）を高めるという視点においては
バックアップ環境の構築やバックアップ取得という観点に目が向くケースが多いが
システムの保全性においてはリストアも重要な要素であることを認識するべきである。

有事の際に重要なシステムをいかに早く正常な状態に復旧させるかという点においては、
運用ルールの作成と定期的な訓練による備えが重要だと考える。

どの会社でもバックアップ環境をしっかり用意していると思いますが、
現場の技術者が「本当にシステム復旧できるのか？」といった不安を抱えていることはありませんか？

そのようなことがないように、日頃から訓練による準備で、有事の際に備えることが必要。

7. Integrity（保全性） バックアップ取得ツール

ツール名	ツール特性
Arcserve UDP Unified Data Protection (UDP) | Arcserve	データ保護と災害復旧を目的とした統合ソリューション 重複排除やデータ圧縮、オンプレ・クラウドなどの多様なバックアップ環境をサポート
Veeam Availability Suite No.1 データ保護 | Veeam Data Platform	データ保護と災害復旧を目的とした統合ソリューション データレプリケーション機能やクラウド環境へのデータ移行・バックアップなどをサポート
Acronis Cyber Protect Acronis Cyber Protect 15	データ保護とサイバーセキュリティを統合したオールインワン型のサイバープロテクションソリューション プロアクティブ・アクティブ・リアクティブ保護機能などが特徴
Cohesity データ保護ソリューション & ソフトウェア | Cohesity DataProtect	データ管理と保護を統合した次世代のプラットフォーム 統合データ管理、スケーラビリティ、AIベースのデータ分類や脅威検知機能などが特徴
NetBackup (1) 新規メッセージ!	エンタープライズ向けのデータ保護ソリューション 統合データ保護、プロセス自動化による運用効率化、スケーラビリティなどが特徴
AWS Backup サービスとしての Backup - 一元化されたバックアップ - AWS Backup - AWS	AWSサービスやハイブリッドワークロードのデータ保護を一元化して自動化するフルマネージドサービス 一元管理、ライフサイクル管理、クロスリージョン管理などが特徴
Azure Backup Azure Backup とは - Azure Backup | Microsoft Learn	Microsoft Azureクラウドプラットフォームを利用したデータ保護ソリューション 一元管理、スケーラビリティ、アプリケーション整合性バックアップなどが特徴

8. Security(安全性) 脆弱性対応方針

Security(安全性)の維持においては、システムの安定稼働を維持するため、脆弱性情報を収集し、適用するためのルールを明確にすることが設計のポイントとなる。
脆弱性対策情報提供サイト(JVN・JPCERT)および各メーカ・ベンダーなどから適宜収集し、
脆弱性対応が必要と判断された場合、速やかにセキュリティパッチの適用を計画することが重要。

参考:CVSS (共通脆弱性評価システム)から脆弱性情報を収集する場合、提供されるスコア値から適用判断する方法がある。

CVSS深刻度レベル

深刻度	スコア
緊急(Critical)	9.0 ～ 10.0
重要(High)	7.0 ～ 8.9
警告(Moderate)	4.0 ～ 6.9
注意(Low)	0.1 ～ 3.9
なし	0

例)深刻度:緊急以上については、システム与える影響度・範囲を取り纏め、対応方針を協議する。

8. Security(安全性) セキュリティパッチ・脆弱性対応期限案

深刻度	対応期限		理由
	社内システム	インターネット公開	
緊急（Critical） CVSS:9.0-10.0	即時（24時間以内）	即時（24時間以内）	攻撃者によって悪用される可能性が高く、システム全体に深刻な影響を及ぼす可能性があるため、迅速に対応が必要
重要（High） CVSS:7.0-8.9	1週間以内	1週間以内	重大度の高い脆弱性がありリスクが高い。即時が難しい場合は、1週間を目途に対応する
警告（Moderate） CVSS:4.0-6.9	1か月以内	1か月以内	攻撃者に悪用される可能性があるものの、影響が限定的であるため、1か月を目途に対応する
注意（Low） CVSS:0.1-3.9	3ヵ月以内	1ヵ月以内	悪用される可能性が低く、影響も限定的。サーバなどの定期メンテナンスタイミングで適用する

※インターネットに公開されているサーバに関しては、外部からの攻撃が受けやすいため、できるだけ迅速に対応することが求められる。

8. Security(安全性) 脆弱性対応 (代替策)

脆弱性対応ができない場合、IT部門の責任者の承認を得て、以下の対応を行う

- 遵守できないセキュリティ要件の洗い出し
- 遵守できない理由
- 想定されるリスクや影響度
- 代替手段の内容
- 代替手段を適用する期間

※予算がないという理由は許可しない。計画的に予算を組むよう提案をする。(予算化できなかった場合は、その部門の責任)

例:

・遵守できないセキュリティ要件
→Webシステムの脆弱性 (Apacheのバージョンアップ)
・遵守できない理由
→システム改修に1年以上かかる想定でるため
・想定されるリスクや影響度
→脆弱性をつかれ、踏み台サーバとして社内システムへアクセスできてしまう
・代替手段の内容
→パーソナルFWでhttp通信を制御 管理コンソールへのアクセスができないよう、管理者権限を特定の人のみとする (アクセス記録をとる)
・代替手段を適用する期間
→2025/1/1-2025/12/31

8. Security（安全性） 脆弱性対応の提言

ITシステムを安心・安全に提供するには事業継続も重要だがSecurity（安全性）を維持する
脆弱性対応が重要である。

IT担当者が、ITベンダーなどからセキュリティ情報を入手し、期日までに対策を適用するための
ルールを運用設計で定義し、組織と徹底させる運用が重要である。
ルールが適用できない場合、セキュリティリスクについて説明し、代替策を必ず策定する。
それでも受け入れない場合は、利害関係者での合意内容をエビデンスとして残しておく。

このような取り組みを組織全体で徹底させる取り組みが必要。

8. Security（安全性） 脆弱性診断ツール

ツール名	得意な機能	メリット	デメリット
JVN　脆弱性対策情報データベース JVN iPedia - 脆弱性対策情報データベース	手動検索	安価	各自で該当する製品から検索が必要なため、時間がかかる
Tanium Tanium: 自律型エンドポイント管理のプラットフォーム	自動適用	プラグインが入っていないサーバを見つけることができ、強制的に導入可能	利用料が高い
Nessus Professional Nessus Professional による詳細な脆弱性評価 | Tenable®	診断可能な脆弱性	プラグインの種類によって、さまざまな診断が可能。 脆弱性データベースが常に更新されている。	プラグインが入っていないサーバは検査できない
Nmap Nmap: the Network Mapper - Free Security Scanner	ネットワーク探索	ポートスキャン機能が充実している オープンソース	linuxはsudo権限が必要 サーバに対し負荷がかかってしまう

9. まとめ

企業活動においてITシステムは業務効率化や生産性の向上、意思決定の迅速化など企業の成長と持続可能な経営に不可欠な要素になってきている。
複雑化、肥大化するITインフラの運用・保守において、技術者への要求・負担も高まっている。

如何に安心・安全・安定的にシステムを運用するか、これからのITインフラの維持、管理に向けては

- 効率化するための有効なツールの活用
- 有事に備えた訓練や準備
- セキュリティ情報の収集および対策の徹底

が必要となる。

これらを運用設計の段階から定義しておくことが重要である。

そのためには運用・保守フェーズの技術者が運用設計にしっかり関与していくことが重要である。