テーマ

最新の環境変化に伴うISMSの実装検討

クラウドファースト時代のリスクマネジメントの事例研究

JNSA 標準化WG
日本ISMSユーザグループ　リーダー
インプリメンテーション研究会　主査

2019年12月4日

魚脇　雅晴

インプリメンテーションWGの活動テーマ

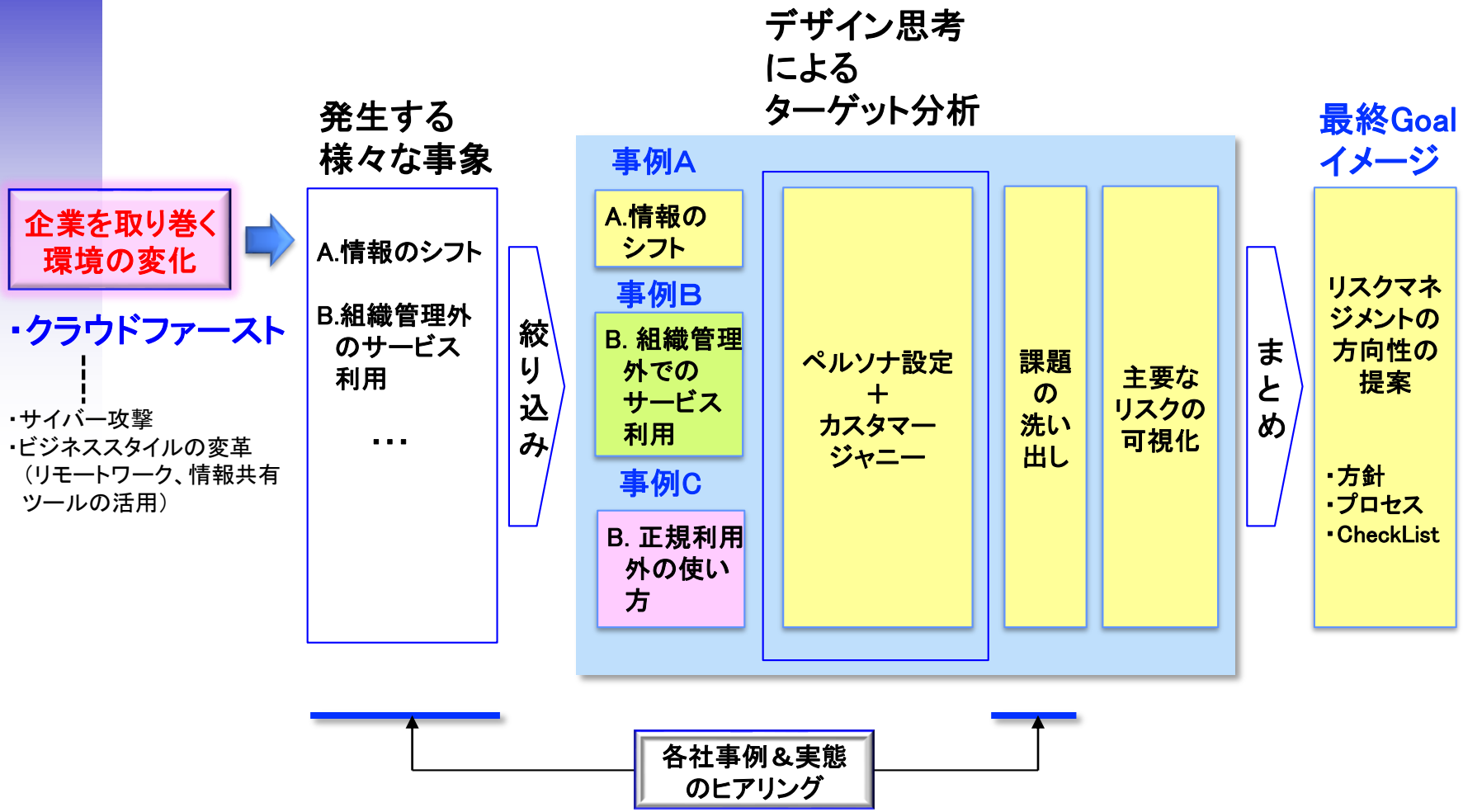
年度	インプリメンテーションWG	メジャメントWG
2006	■本WGの活動紹介＆ISMS導入に関する課題の事例紹介	■有効性測定の基本的な考え方＆取り組み事例紹介
2007	■情報セキュリティ研修・啓発 ■効率的リスクアセスメント	■有効性測定の基本的な考え方＆新たな取り組み事例紹介 （進捗状況含む）
2008	■ISMS構築事例に見る有効性測定構築の傾向 ■業務委託先のセキュリティ評価	■有効性測定の基本的な考え方＆共通フレームワーク案 （進捗状況含む）
2009	■標準的なリスク分類と具体的な管理策の対応のモデル化 ■管理策の有効性評価を効果的に行うモニタリング手法のモデル化	■ISO/IEC27001における「有効性測定」
2010	■標準的なリスク分類と具体的な管理策の対応のモデル化 ■管理策の有効性評価を効果的に行うモニタリング手法のモデル化	■ISO/IEC27001における「有効性測定」
2011	■可視化手法を用いたリスク対策モデル ■ISMS全体の有効性評価手法	■管理策の有効性測定
2012	■可視化手法を用いたリスク対策モデルとその実践的応用 ■ISMS実践手法　BCPのモデル化の検討	■管理策の有効性測定
2013	■ISMS推進事務局の悩みと解決策 ■有効性評価に基づくISMS実践活用	
2014	■ISMS推進事務局の悩みと解決策 ■ISMS規格改訂にともなう実装方法の検討	
2015	■ISMSを成功させる理想的なCISOの条件 ■減らないインシデントの特効薬	
2016	■サイバー攻撃を事例としたリスクマネジメントの実践 ■運用フェーズにおける有効性の評価	
2017	■現場と連携したリスクアセスメント手法の実践活用 ■内部監査を有効に運用するための手法の考察	
2018	■ISMS規格要求事項から紐解く最新のビジネス環境リスク ■働き方改革における情報セキュリティ	
2019	**■テーマ1 ・・・最新の環境変化に伴うISMSの実装検討** **■テーマ2 ・・・ISMSの管理策の実装**「イベントログについての考察」	

インプリメンテーション研究会のメンバー

橋本　秀行	ＫＤＤＩ株式会社
森　親章	NECソリューションイノベータ株式会社
大熊　信也	NECソリューションイノベータ株式会社
大平　泰寛	NECソリューションイノベータ株式会社
魚脇　雅晴	NTTコムソリューションズ株式会社
原　路子	NTTコムソリューションズ株式会社
広田　正毅	NTTコムソリューションズ株式会社
村山 尚	NTTコムソリューションズ株式会社
中谷　勝彦	NTTコムソリューションズ株式会社
徳永　安芸	NTTコムソリューションズ株式会社
梅　文夫	NTTコムソリューションズ株式会社
中村　昌登	アイレット株式会社
早川 宏	エヌ・ティ・ティ・コミュニケーションズ株式会社
小澤　隆一	エヌ・ティ・ティ・データ先端技術株式会社
今野　尚昭	エヌ・ティ・ティ・データ先端技術株式会社
鍋島　聡臣	エヌ・ティ・ティ・データ先端技術株式会社
松原　勝美	株式会社インターネットイニシアティブ
和田　義毅	株式会社エヌ・ティ・ティ・データ
間形　文彦	日本電信電話株式会社
小梁　康志	リコージャパン株式会社

羽田　卓郎	リコージャパン株式会社
矢島　大	リコージャパン株式会社
今井　岳彦	リコージャパン株式会社
置田 健児	リコージャパン株式会社
帯刀　静夫	株式会社NTTファシリティーズエンジニアリング
宮本　俊之	株式会社NTTファシリティーズエンジニアリング
上村 竜也	株式会社VSN
宮本　豊	株式会社ラック
槇谷　努	富士通株式会社
阿部　正峰	富士通株式会社
新井 雅	富士通株式会社
増田　浩次	富士通株式会社
小野　等	個人会員
尾崎 幸彦	個人会員
冨田　吉弘	個人会員
野代　安紀	個人会員
葛西　章広	個人会員
秋山　健一	個人会員（NECプラットフォームズ株式会社）
松居　隼司	個人会員（NECプラットフォームズ株式会社）
安田　次郎	個人会員（NECプラットフォームズ株式会社）

最新のビジネス環境変化に伴うISMSの実装検討の進め方



テーマ選定の背景

最新の環境変化に伴うISMSの実装検討

クラウドファースト時代のリスクマネジメントの事例研究

企業を取り巻く環境の変化

- ・クラウドファースト
  - ・サイバー攻撃
  - ・ビジネススタイルの変革（リモートワーク、情報共有ツールの活用）

大きな環境の変化起こっているが、従来通りのISMS管理策の実装のままで対応出来ているのか？？？

- 不足しているものは何か？
- 従来の枠組みに＋αするものは何か？（ISO/IEC27001＋27017）
- ビジネスとセキュリティのバランスは？

企業を取巻く環境変化・・・　クラウドファーストの流れ

下記のような様々な理由から**初期投資のいらないサービス利用型のクラウドへのシフトが加速**している。
一方でコンプライアンスや機密性の問題から全てをクラウドに移行できないとする企業も存在し、並存する運用が模索されている

- **ビジネスの変化に対する対応へのスピードアップ**
- **ICTコストの削減**
- **業務効率（生産性）向上**
- **事業継続対応**
- **技術者不足への対応など・・・**

「クラウド・バイ・デフォルト原則」

政府情報システムにおけるクラウド サービスの利用に係る基本方針
https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf

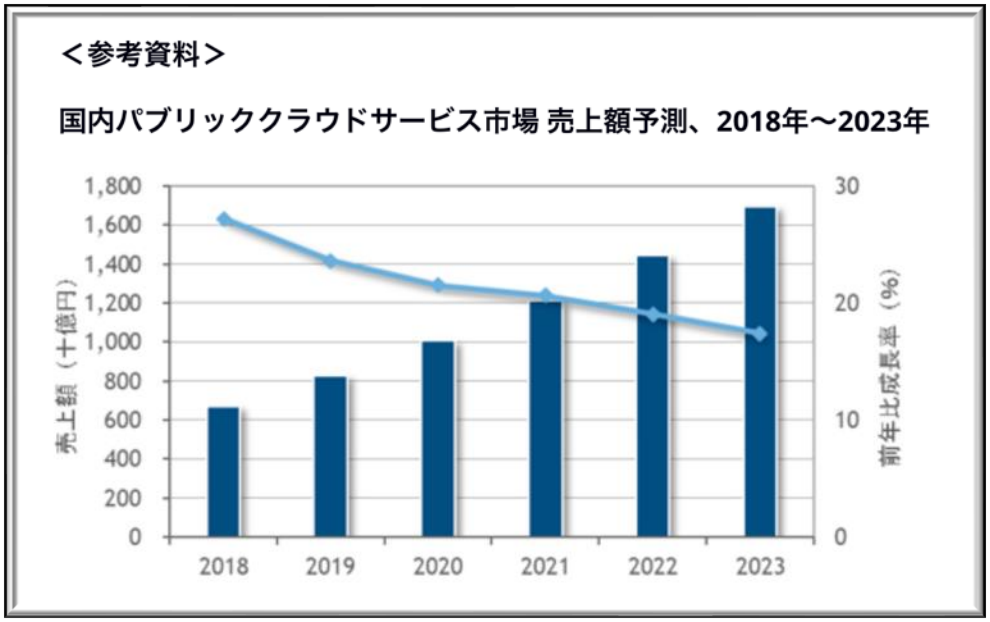
（参考） クラウドとオンプレの比較表

比較項目		クラウド	オンプレ
コスト	初期	◎	×
	ランニング	○	○
リードタイム		○	×
運用の手間		○	×
事業継続		○	×

参考：パブリッククラウドサービス市場の拡大

・2018年の国内パブリッククラウド市場は、前年比27.2%増の6、688億円となった
・2018年～2023年の年間成長率（CAGR：Compound Annual Growth Rate）は20.4%で推移
・2023年の市場規模は2018年比2.5倍の1兆6,940億円になるとIDCは予測

・今後も、ユーザ企業における**従来型ITからパブリッククラウドへの移行は継続**
・DXや新技術を活用した**「生産性向上」「業務の効率化」を目的**としてクラウドの利用が増加
・今後も**高い成長を継続**すると予測



https://www.idc.com/getdoc.jsp?containerId=prJPJ44928319

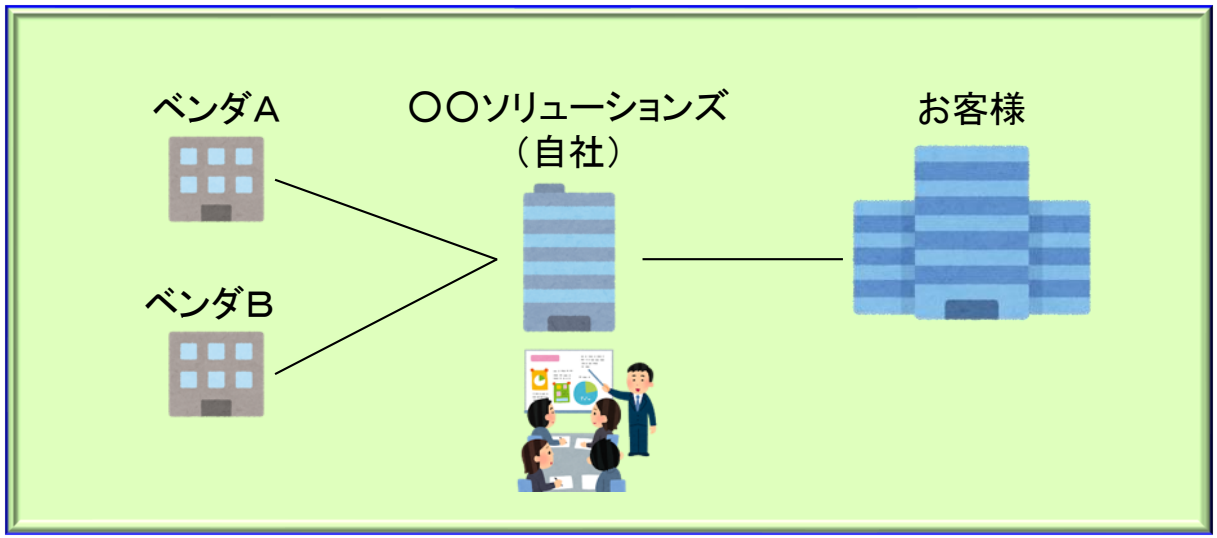
テーマの狙いと検討のアプローチ

今回のテーマを分析＆検討を進める上で下記の取り組みを実施する。

- **従来のISMSの運用の枠組みで不足しているもの（＋α）を可視化**する
- 特定の企業の業種や業態をモデル設定し、**デザイン思考での課題の深堀り**する
- 上記の内容をインプット情報としてリスクアセスメントを実施

○企業設定（○○ソリューションズ株式会社）

- 業種/規模：中堅のIT企業、社員1000名
- 企業動向　：これまではオンプレの開発がメインだったが、昨今はクラウド上での開発＆運用がメインとなってきている。取引ベンダもクラウドの構築などがメインの会社に主軸が移ってきている。それに伴い仕事のやり取りもメールベースからコミュニケーションツールに移行されつつある。



情報セキュリティの世界にデザイン思考の考えを導入・・・

デザイン思考を利用したターゲット分析のアプローチ

○ペルソナを設定する理由は？

ユーザを詳細な仮想ユーザ『ペルソナ』として厳密に設定し、そのペルソナをターゲットに分析 を行うことにより、分析対象のターゲットを明確にするとともに検討メンバーでの共同作業において共通認識を持って分析がぶれずに出来る

→ペルソナがどのような行動をとるのかカスタマージャーニーで洗い出しを行い、なぜそのような行動をとるのか分析する

○ユースケースではダメなのか？

内部構造ではなく外部から見た機能に着目して「どのように利用できるか?」という側面について考えるため、機能面や網羅性を求める平均点となってしまうので、詳細な分析や共同作業についてはペルソナの方が適している

事例研究を深掘りするためのペルソナ設定

ルールを作る立場

・ISMS事務局員
・規則　守（45歳）男性、既婚

・**会社の情報を守るのに生きがい**を感じているが、昨今のクラウド利用等で**情報が外部に保管されている状況を憂い**ている・・・

・45歳男性、既婚、妻（43歳）、娘（高1）、息子（中2）
・役職（課長代理）
・年収650万
・大学卒業後、中堅のIT企業に入社後SIビジネスに従事していたが誠実な性格や困難なプロジェクトでもやり抜く実行力から会社全体のセキュリティ業務に従事することになる
・セキュリティ第一主義ではなく、常に現場の課題に目を向けてビジネスとのバランスを考えている
・会社ではビジネスのスピードを重視し、クラウドへのシフトを加速しており、メリットを認める傍に目に見えないリスクを懸念している

ルールを遵守する立場

・お客様SI案件のPM
・唯我独尊（32歳）男性、未婚

・日頃から**セキュリティ重視の流れに不満**を募らせている。ビジネスを優先するためなら**多少のルール違反は必要**と考えている・・・

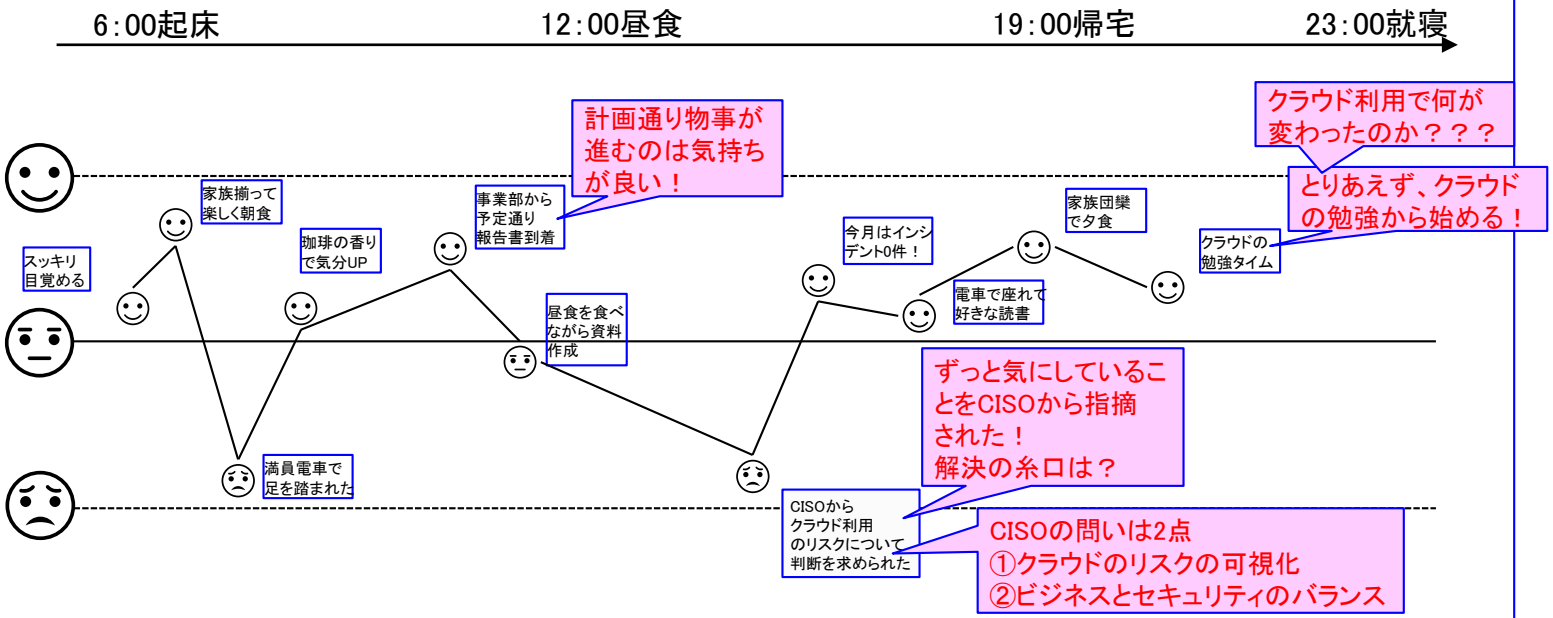
・32歳男性、未婚
・役職（主任）
・年収500万
・大学卒業後、中堅のIT企業に入社後SIビジネスに従事、学生時代から身につけていたプログラミングスキルを発揮して様々なソリューションを提供
・最近はクラウドサービスを利用したSI案件を提案＆構築をPMとして実施
・案件の仕様調整などをメールで実施するには制限が多く、コミュニケーションツール等の導入でスピードアップを模索している
・社外とのコミュニティ活動にも熱心に参加

カスタマージャーニー （規則 守さんの1日）

ルールを作る立場

・ISMS事務局員
・**規則　守**（45歳）男性、既婚

・**会社の情報を守るのに生きがい**を感じているが、昨今のクラウド利用等で情報が外部に保管されている状況を憂いている・・・

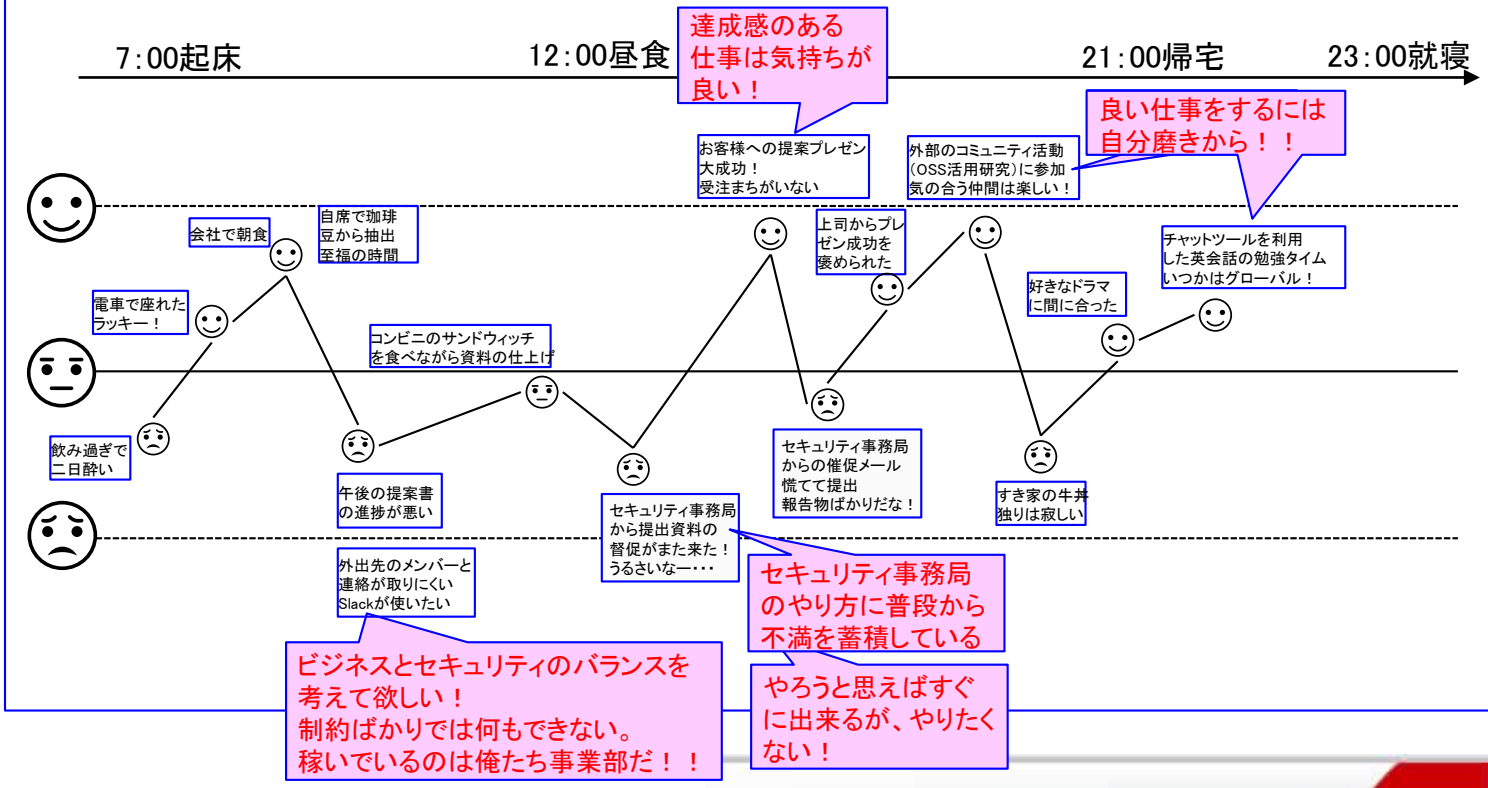


カスタマージャーニー （唯我独尊さんの1日）

ルールを遵守する立場

・お客様SI案件のPM
・**唯我独尊**（32歳）男性、未婚

・日頃から**セキュリティ重視の流れに不満**を募らせている。ビジネスを優先するためなら**多少のルール違反は必要**と考えている・・・



クラウド導入に関する経営層の考え

クラウド化はどんどん進めるが、
リスクは負いたくない！

世の中全体の流れとしてオンプレ中心から急速にクラウド化が進んでいるため、我が社としても大きくクラウド化へ舵を切る必要がある。**クラウドには様々なメリット**があるが、光と陰のような関係で**見えていないデメリット**もあるはずだ。

だが、現時点でビジネスとセキュリティのバランスをどのように設定するか明確な判断基準はない。仕方がないので、**推進派と制限派の意見を戦わせることでリスクの可視化と課題への対応を明確**にすることとした。

唯我独尊さん　心の声

対比

心の声

規則守さん

経営方針の伝達・・・マネジメント層の指示

経営方針

クラウドファーストで
ビジネスのスピードアップ

経営層

指示事項

・クラウドファースト
・ビジネススピードアップ
・ビジネススタイル変革

指示事項

・クラウドファースト
・セキュリティとビジネスのバランス
　を取れ！

事業部

・お客様SI案件のPM
・唯我独尊（32歳）
　男性、未婚

経営企画部

・ISMS事務局員
・規則　守（45歳）
　男性、既婚

唯我独尊さんの心の声

・クラウドファースト
・ビジネススピードアップ
・ビジネススタイル変革

ビジネスのスピードをアップさせる
にはまずは**メールではなく情報共有ツールの導入**から始めるか・・・

ビジネスのスタイルを変革するには
クラウド中心に業務を変えて、**サプライチェーンとしてお客様や委託先も含めた変革が必要**だ！

・お客様SI案件のPM
・唯我独尊（32歳）
男性、未婚

ビジネス優先で考えれば**面倒な社内手続き（リスクアセスメント）は、無視**して導入しよう！

規則 守さんの心の声

・クラウドファースト
・セキュリティとビジネスのバランス
　を取れ！

クラウド化によって**何が起きているのかまずは現場を調査**することから始めてみよう！

経営層からは「セキュリティとビジネスのバランスを取れ！」と言われたが・・・
バランスがとれるのかなぁ？

・ISMS事務局員
・規則　守（45歳）
　男性、既婚

ルールを守らない人が多いので制限する方が楽なんだけど

クラウドの**管理基準ISO/IEC27017の適合チェックは以前から実施**しているから大丈夫なはずなんだけど・・・

クラウドの管理基準に基づくチェックリストでチェック済み！

規則 守さんの心の声・・・可視化出来ていないリスクは？

・ISMS事務局員
・規則　守（45歳）
男性、既婚

クラウドの**管理基準ISO/IEC27017の適合チェックは以前から実施**している
から大丈夫なはずなんだけど・・・

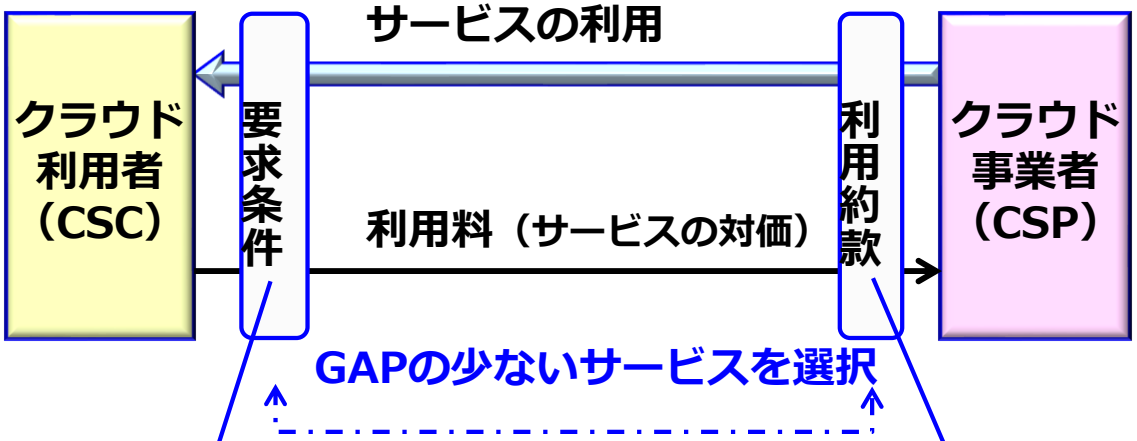
我社はすべてのクラウドサービス
の導入時にクラウドの管理基準に
基づくチェックリストでチェックして
いるのでリスクはコントロール
出来ている！

ISO/IEC27017の対応だけで十分か？

可視化出来ていないリスクは無いのか？？？

参考：クラウドサービス要件の確認事項（ISO/IEC27017）

サービス要件の確認＆GAPの可視化を実施（サービス利用の観点）



○機能要件
オートスケーリング、DRサイト・・・
○サービス/運用管理
稼働率、故障通知・・・
○コンプライアンス
個人情報保護、法廷闘争・・
○セキュリティ要件
暗号化、アクセス権/ログ管理・・
等々

クラウド事業者の提供サービス
＋
α 利用者側にて不足分を補完

利用約款に基づくサービス提供形態

○機能要件
○運用管理
○コンプライアンス
○セキュリティ要件
等々

クルマに例えれば、安心安全なクルマは事故が起こらないか？

安全運転

×

安心・安全なクルマ

＝

安心・安全なものでも
使い方次第で事故が起こる！

あおり運転
信号無視

×

安心・安全なクルマ

＝

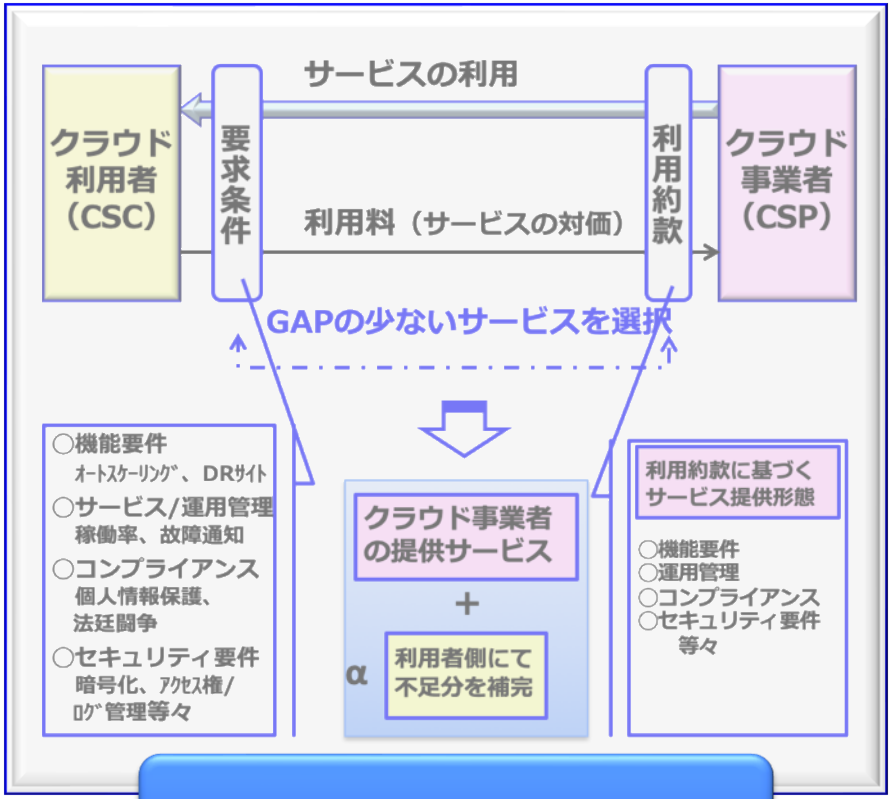
事故

クラウドサービスの利用形態に着目した確認が必要？

クラウドサービスを安全に利用するためには？

利用形態

クラウドサービス



・どう使うか？何に使うか？

・利

・誤

・社外

クラウドサービスの利用形態に着目した確認が必要！

クラウドファーストで現場で何が起こっているか？

企業を取り巻く環境の変化

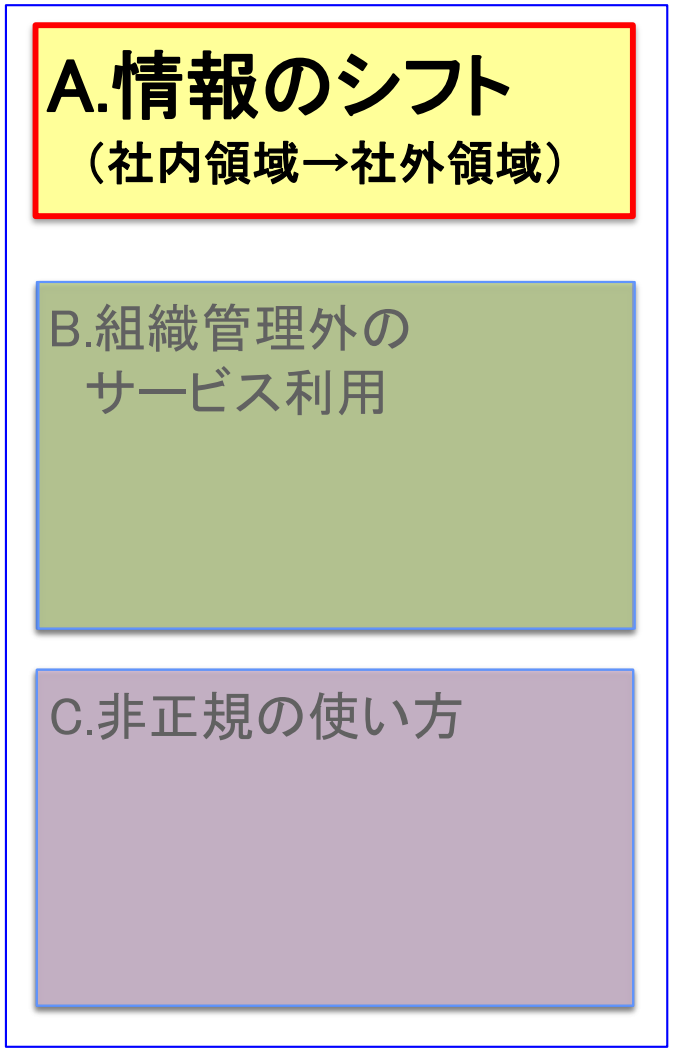
結果として何が起きるか？

・クラウドファースト

・サイバー攻撃
・ビジネススタイルの変革
（リモートワーク、情報共有ツールの活用）

分類	発生事象	ブレークダウン
A.情報のシフト （社内領域→社外領域）	**情報管理が曖昧** →厳格に管理すべきところ、社内管理と同じやり方（同レベル）の管理方法となっている	事例A
B.組織管理外のサービス利用	**野良クラウドなど組織で管理出来ていないサービスの蔓延** →存在の有無が把握出来ていない！ →利用実態も不明！ （数、利用形態など）	事例B
C. 非正規の使い方	**承認された範囲外での利用や誤用によるリスク** →社外（客先/委託先）からアクセス！ →私有PC/スマホによる無断使用！ →許可されたプロジェクト以外での拡大利用（無承認） →勝手な個人情報などの保管 →管理責任者の不在、管理の有名無実化	事例C

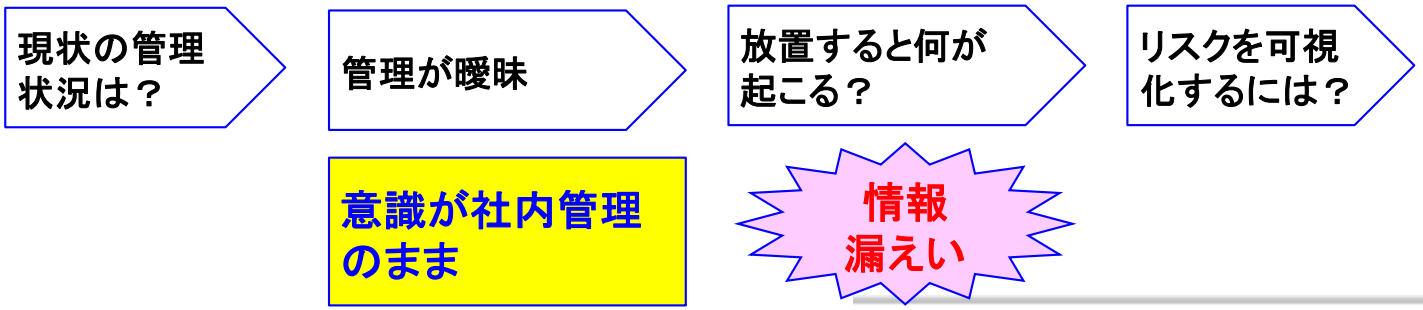
事例 A



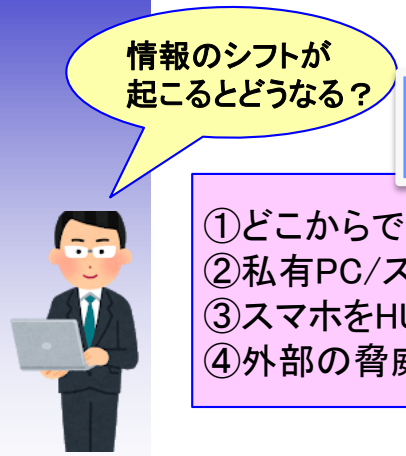
社内領域→社外領域

クラウドサービス利用時における課題の認識

NO	分類	発生事象	現状＆課題
A	情報のシフト （社内領域→社外領域）	**管理が曖昧** 厳格に管理すべきところ、社内管理と同じやり方（同レベル）の管理方法となっている	クラウドファーストで情報がどんどん社外に持ち出されているが、**管理方法は社内で保管していた時と変わらない** **→利用実態が把握出来ていない！** ・情報が可視化されにくい（何が、何処に、どのように管理） ・利用しているクラウドサービスの区別のみ **→管理者の意識レベルが社内管理のまま？** ・オンプレの場合は社内限定が当たり前の世界だったが、クラウドでは共有設定を誤ると社外からも自由にアクセス可能となってしまう ・クラウドサービスのアクセス権管理者の意識が社内管理のまま **→ID/PWDがあれば会社PC以外でも利用可能** ・管理実態が把握しにくい



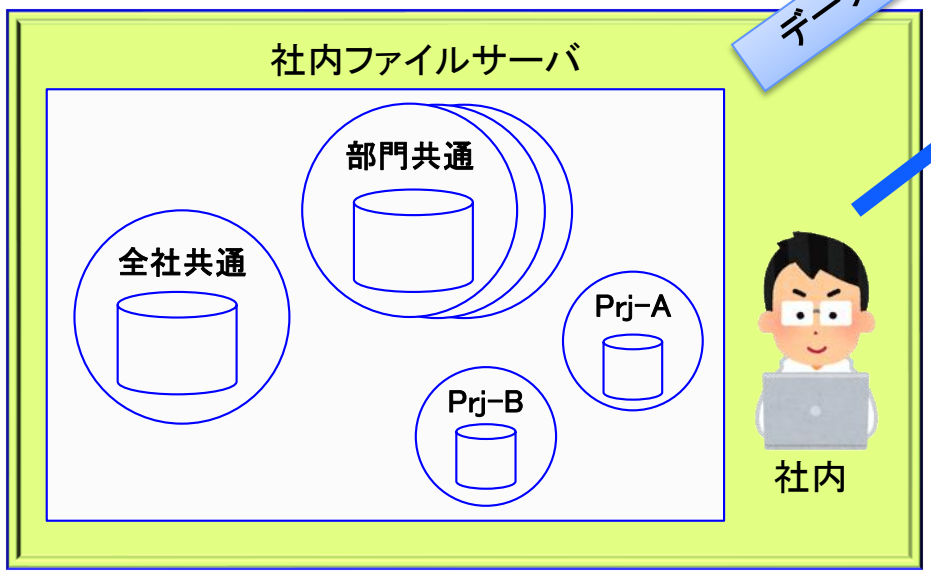
情報のシフト（社内 → 社外）で起こること・・・

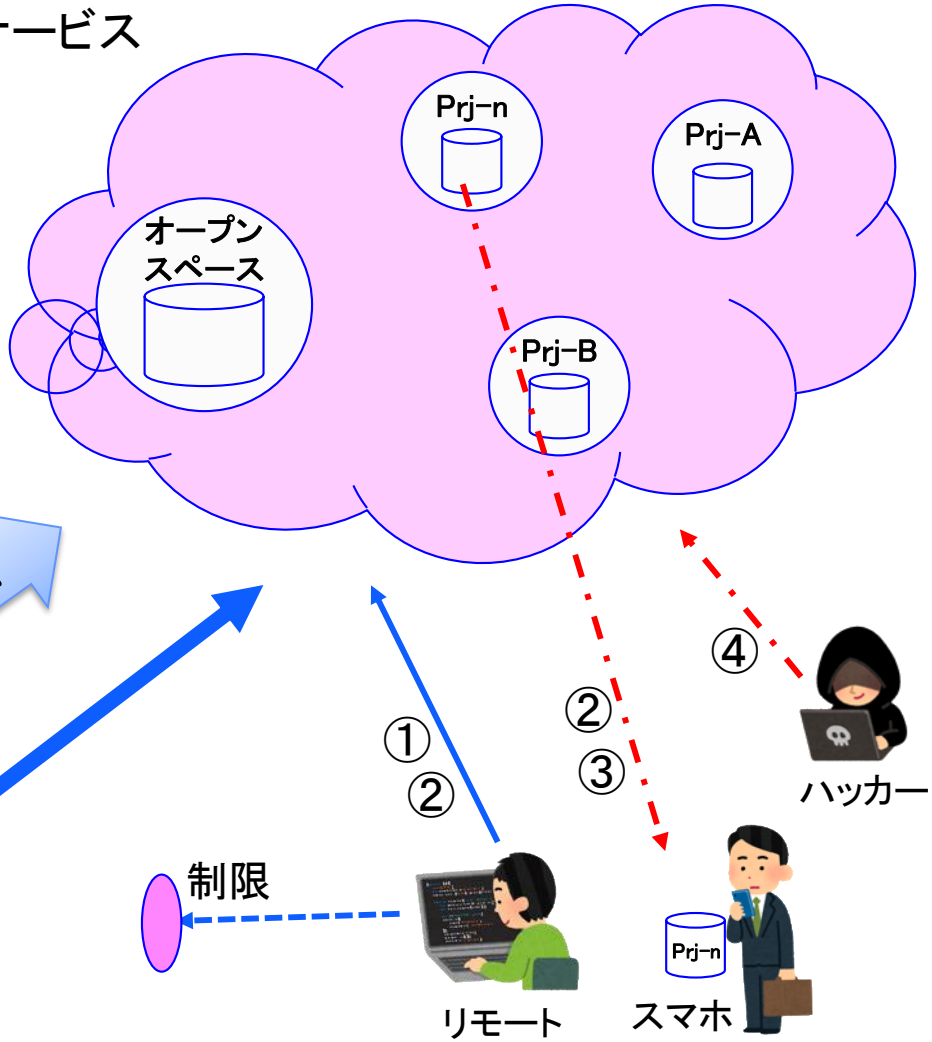


情報のシフトで起こっていることを中心に記載する

①どこからでもアクセス可能
②私有PC/スマホからもアクセス可能
③スマホをHUBにして情報持ち出し可能
④外部の脅威に常に晒されている

・ISMS事務局員
・規則　守（45歳）
男性、既婚





事例A（X社）：情報資産台帳上でのクラウド保管情報

・ISMS事務局員
・規則　守（45歳）
男性、既婚

管理実態を調査してみよう！

情報資産台帳で管理できている情報は下記の通り
従来通り（社内管理）の枠組みで守れるのか？

・保存管理　　：外部サービス（ASP/cloud）に情報を保管
・アクセス権管理：情報にアクセス可能なグループの特定
・流通管理　　：社内、社外への情報流通の有無

※：懸念点

＊1：サービス利用時の保管場所やアクセス権管理の管理者が誰かが明確になっていない？
＊2：クラウドサービスによって管理方法やアクセス権限の利用者への移譲範囲が異なる
＊3：実際の利用実態を把握する手段が無い

一般機密情報			個人情報関連する管理情報							保存管理		アクセス権管理		流通管理		
情報			個人情報							保存管理		アクセス権管理		流通管理		
業務別の情報の特定	個人情報の有無	CIAの観点での情報資産価値の特定	項目	利用目的	取得元	取得手段	件数	開示対象	要配慮	保管期限	保管場所	アクセスG#1 AWS#1	アクセスG#2	送付なし	社内送付	社外
	○										FS	該当選択			主な手段	主な手段
											社内SYS				代替手段	代替手段
											社にPC					
											ASP/cloud	○				
											外部媒体					
											書庫					

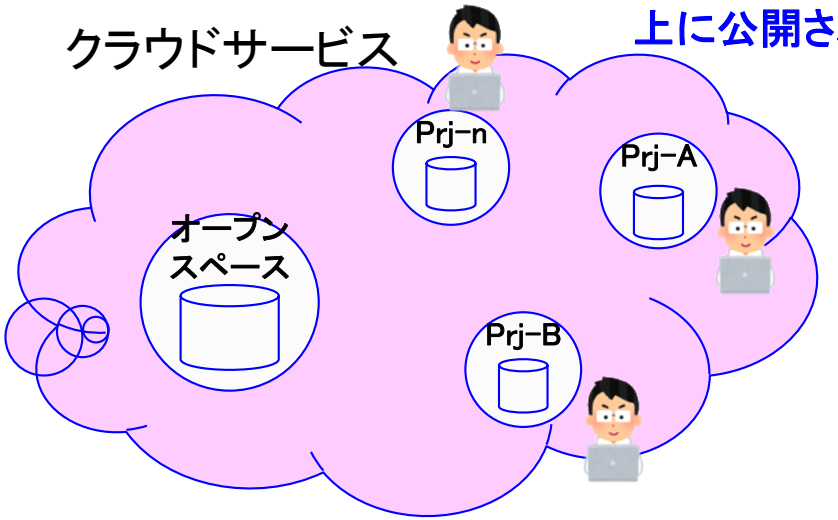
情報の管理方法について記述

個人情報有りの時に関連する情報を追記

管理者の意識が社内で保管していた時のまま？・・・

管理内容として十分か・・・？

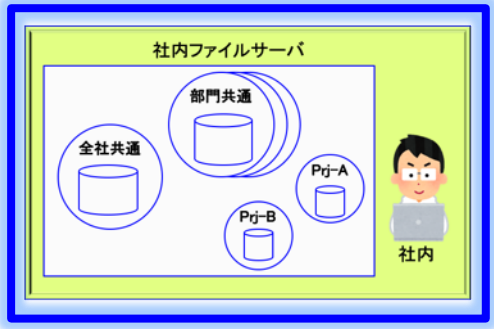
情報資産台帳



台帳で管理出来ている項目

管理責任	情報資産管理簿毎の管理者
保存管理	どのクラウドを利用しているか
アクセス権管理	保管されている情報にアクセス可能なグループ
流通管理	社内/社外への情報流通の有無

検証作業



社内限定の
閉空間

事例検証：情報資産台帳上でのクラウド保管情報

クラウド上に保管された情報資産の管理方法はオンプレと同じレベル

管理レベル（現状）

管理区分	管理状況（現状）
管理責任	情報資産管理簿毎の管理者
保存管理	どのクラウドを利用しているか
アクセス権管理	保管されている情報にアクセス可能なグループ
流通管理	社内/社外への情報流通の有無

オンプレの場合

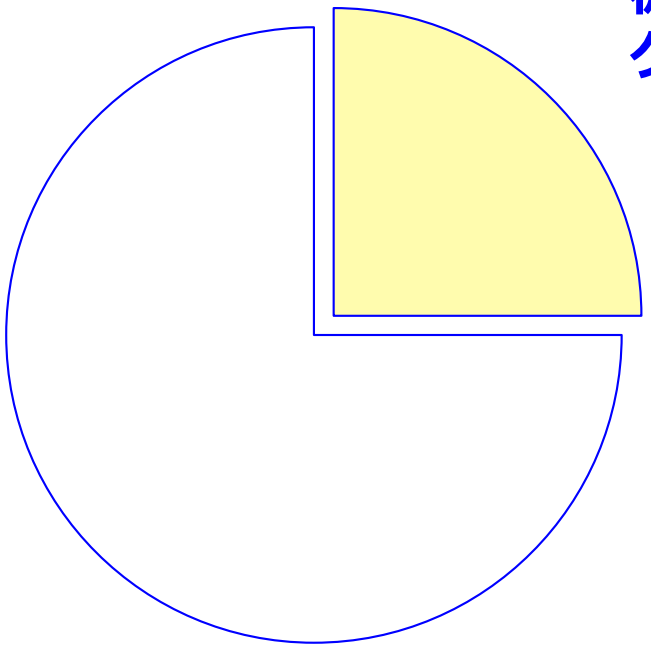
・組織フォルダへのアクセス制限はAD連携し、組織単位でのアクセス制御
・複数の組織がまたがるPJフォルダは個別に管理者が設定する運用
※：アクセス権の付与が若干曖昧だとしても社内からのアクセスに限定されているために外部からの不正なアクセスのリスクは少ない。
（**ずさんな管理を実施していても自社の管理下**）

クラウドの場合

・仮想空間やワークスペースという概念で管理し、アカウント単位で許可された仮想空間にアクセス可能（保管場所が不明確：どの仮想空間か？）
・ID/PWDの認証後は仮想空間内を自由にアクセス可能
・厳密に管理しないとフルアクセス状態となっていることが懸念
（間違った相手にフルアクセスを付与して情報漏洩に繋がったり、ID/PWDの管理があまいと外部からの侵入される）
・**アクセス権管理の管理者が誰か明確でない**（ワークスペース単位）
・クラウドサービス毎に**アクセス権限の利用者への移譲範囲やデフォルト設定が異なる**
・**従来の流通手段では管理出来ない**
（通常はメールや外部媒体やファイル共有サービスが考えられるが、クラウドサービスの場合の情報流通としては直接アクセス権限の付与の可能性が高い）

事例Aから導かれる分析＆課題

情報のシフト（クラウド保管＆利用）による管理要件の変化



従来の管理方法では十分では無い！
クラウド特有の管理要件とは？

◎ クラウド時代の情報管理
＆ 管理プロセス

- アクセス権管理の管理者が不明確
  （ワークスペース単位）
- 管理者の役割が有名無実化
- クラウドサービスによって仕様が異なる
  （管理方法やアクセス権限の利用者への
  移譲範囲）

事例 B

A.情報のシフト
（社内領域→社外領域）

B. 組織管理外のサービス利用

C.非正規の使い方

クラウドサービス利用時における課題の認識

NO	分類	発生事象	現状＆課題
B	組織管理外のサービス利用	野良クラウドなど組織で管理出来ていないサービスの蔓延	組織として管理されていないクラウド利用の蔓延 **事例紹介** **→野良クラウド利用（個人契約など）の蔓延** ・利用していることに気が付かない **→正規クラウド含めて利用実態が不明（数量、利用目的、利用形態など）** ・クラウドサービスの実態が管理出来ていない（システム管理台帳の対象外となっている） **→目的外利用（これも野良クラウド）** ・検証や研修用のクラウドで商用サービス利用 **→リスクアセスメント未実施のクラウド利用** ・組織として管理されていないので、リスクアセスメントのプロセスが実行されない

野良クラウドの定義と分類

○野良クラウドの定義

組織の情報システム部門が導入や運用を把握していないクラウドのこと。
ローグ(Rogue)は"離脱した"という意味であり、"野良"と意訳された。

○野良クラウドのリスク(落とし穴)

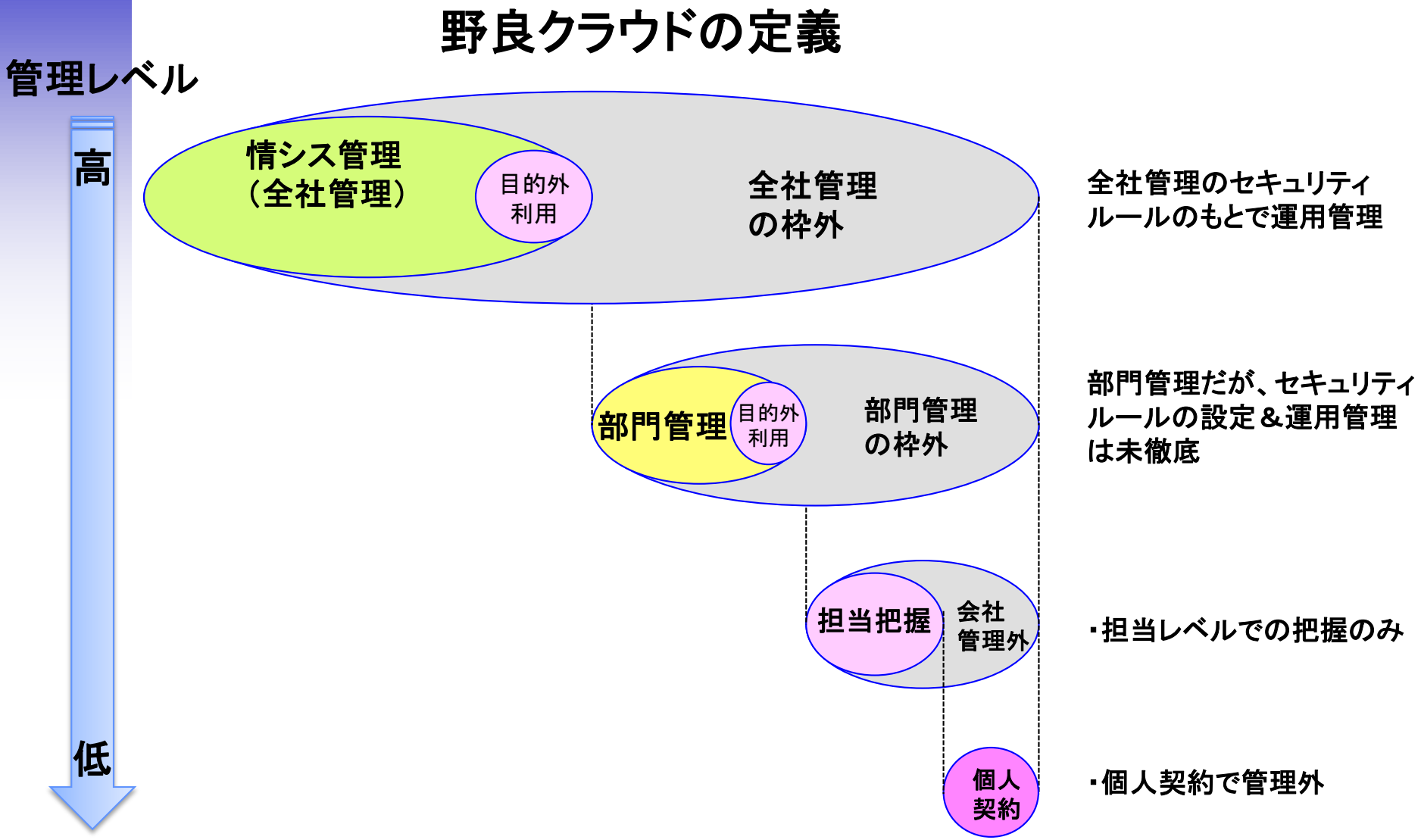
クラウドコンピューティングサービスは、小規模、低価格での導入や運用を行うことが可能なため、各部門や組織内の個人が情報システム部門を通さずに利用している場合もあり、組織の情報セキュリティポリシーが遵守されないことによる機密情報の漏えいリスクが生じるなどの管理上の問題が指摘されている。

http://www.bbtower.co.jp/bbtower-report/technical-term/na/rogue_cloud/

野良クラウドの分類

管理主体	情シス管理 (全社管理内)	部門管理 (全社管理外)	担当(個人) (組織管理外)	個人契約分 (会社管理外)
費用管理	会社負担(無料枠での利用ケースも有)			個人
野良クラウド判定	正規	野良	野良	野良

野良クラウドの定義と管理レベル



野良クラウドの定義（自社管理外のクラウド）

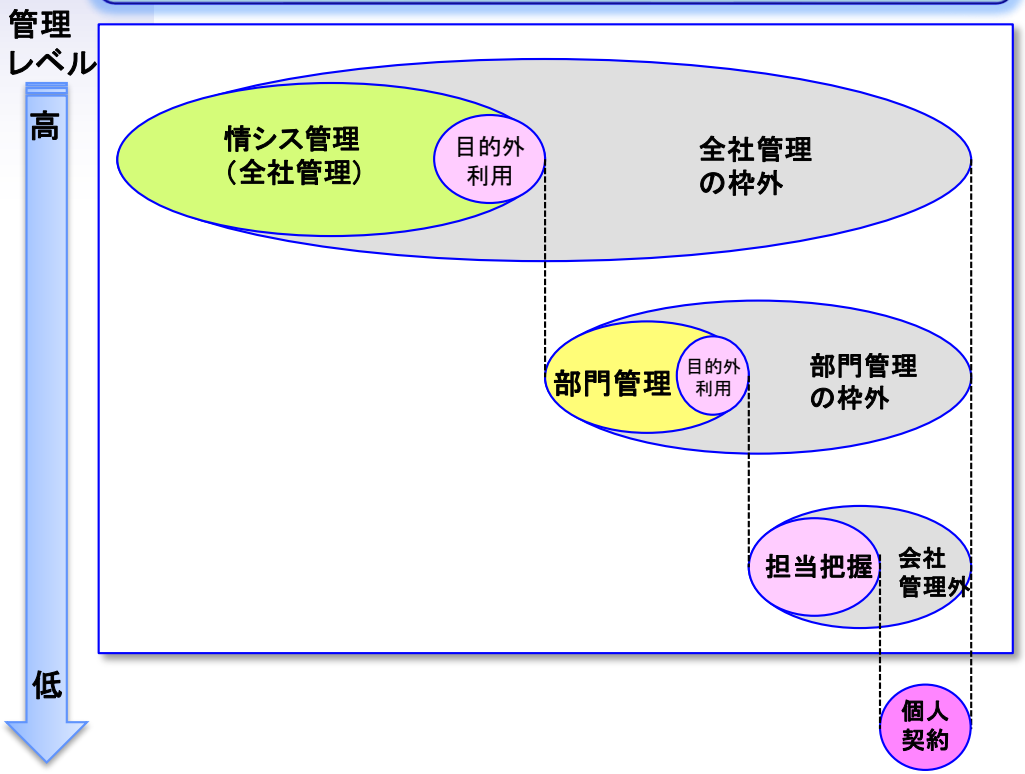
見落としがちな自社管理外のクラウド利用

利用形態（1）

利用形態（2）

自社管理のクラウド

自社管理外のクラウド



自社管理のクラウド

- 意外と多い利用形態
- 管理主体は他社
- 管理責任が不明確

お客様指定
&
親会社指定

自社管理外クラウドの責任について

利用形態（2）

自社管理外のクラウド

・意外と多い利用形態
・管理主体は他社
・管理責任が不明確

お客様指定
&
親会社指定

自社管理外の
クラウド利用でも
責任は発生する！

委託先としての独自
のガイドライン策定など
の自己防衛が必要！

・PWD管理が甘いとハッキング
されて情報漏えいに繋がる！

・事故が発生した場合は誰の責任？
・利用マニュアルや制限事項を 提示されていない
・利用していることを組織として 認識できていない

野良クラウドのリスクとカテゴリ分類

○野良クラウドのリスク（落とし穴）

- 組織の情報システム部門が導入や運用を把握していないクラウド
- 組織の情報セキュリティポリシーが遵守されないことによる機密情報の漏えいリスクの増大
- 利用状況が見えない（存在の有無がわからない・・・）

野良クラウドのカテゴリ分類

カテゴリ	1		2		3	4
管理主体	情シス管理（全社把握）		部門管理（情シス未把握）		担当（個人）把握（組織管理外）	個人契約分（会社管理外）
管理レベル	リスクアセスメント実施	リスクアセスメント未実施	リスクアセスメント不十分		リスクアセスメント未実施	リスクアセスメント未実施
利用目的範囲内外	利用目的内	利用目的外	利用目的内	利用目的外	未承認	未承認
費用管理	会社負担（無料枠での利用ケースも有）					個人
野良クラウド判定	正規	野良	野良	野良	野良	野良

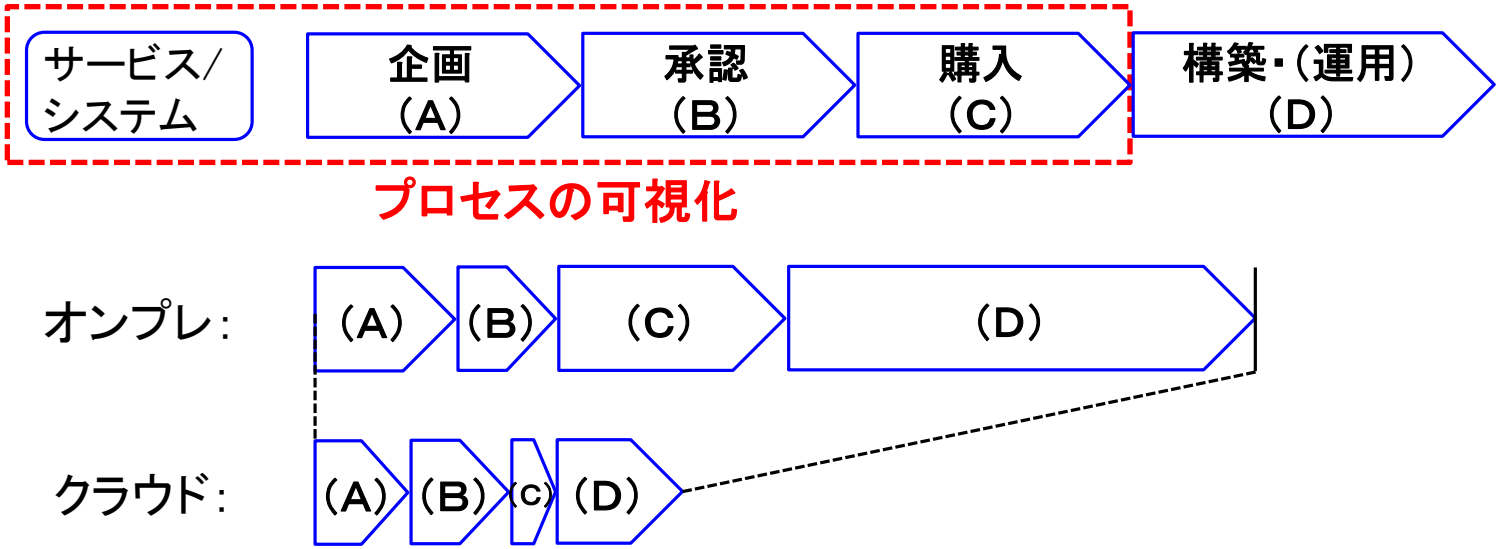
大 ← 組織としてのコントロール → 小　組織管理外

野良クラウド発生メカニズム（クラウドのメリットと課題）

○クラウド利用/サービス利用の特徴と課題

メリット：**すぐに使える**（申込日から使える）、**運用コストが少ない**

課題　　：実体として物が見えないので管理がしにくい
・オンプレのようにデータセンタやサーバルーム等で把握出来ない
・コスト管理でも**実態との関連付けが見えにくい**
（クレジット払いなど）



※：1年間のお試し無料枠もあるので、野良クラウド状態を招きやすく、
実態把握等の管理が難しい

野良クラウド発生メカニズム（正規の手続きの抜け穴）

正規の社内手続きをしなくても利用することが可能・・・

正規の手続きは面倒くさい！

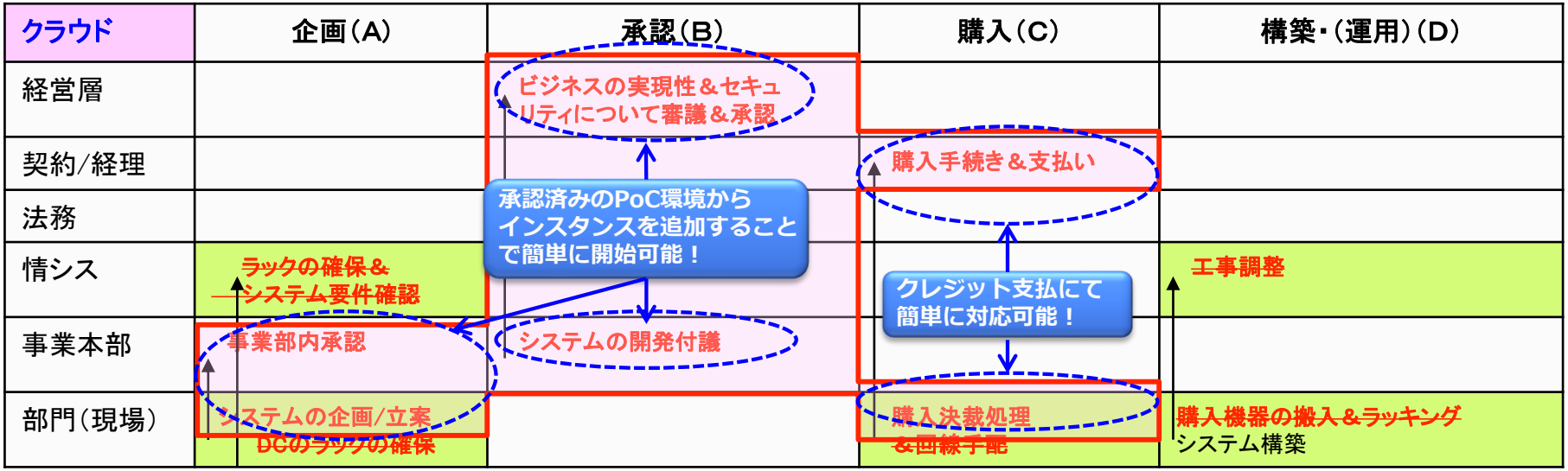
○利用開始の承認手続きをしなくても気がつかない

- 他部との調整が不要（ラック＆回線確保不要）
- クレジットでの支払いが可能＆利用料が少額（部門内で完結、お試し利用等）
- 検証環境からサービス利用への移行も簡単＆瞬時

○野良クラウド（正規の承認なし＆個人契約等）を把握するのが難しい

- 利用開始前に把握することも運用フェーズでも難しい

○正規の手続きしかリスクアセスメントプロセスを通過しない



事例B：サービス利用時における野良クラウド （カテゴリ4）

野良クラウドの分類

カテゴリ	1		2		3	4
管理主体	情シス管理（全社把握）		部門管理（情シス未把握）		担当（個人）把握（組織管理外）	個人契約分（会社管理外）
管理レベル	リスクアセスメント実施	リスクアセスメント未実施	リスクアセスメント不十分		リスクアセスメント未実施	リスクアセスメント未実施
利用目的範囲内外	利用目的内	利用目的外	利用目的内	利用目的外	未承認	未承認
費用管理	会社負担（無料枠での利用ケースも有）					個人
野良クラウド判定	正規	野良	野良	野良	野良	野良

大 ← 組織としてのコントロール → 小

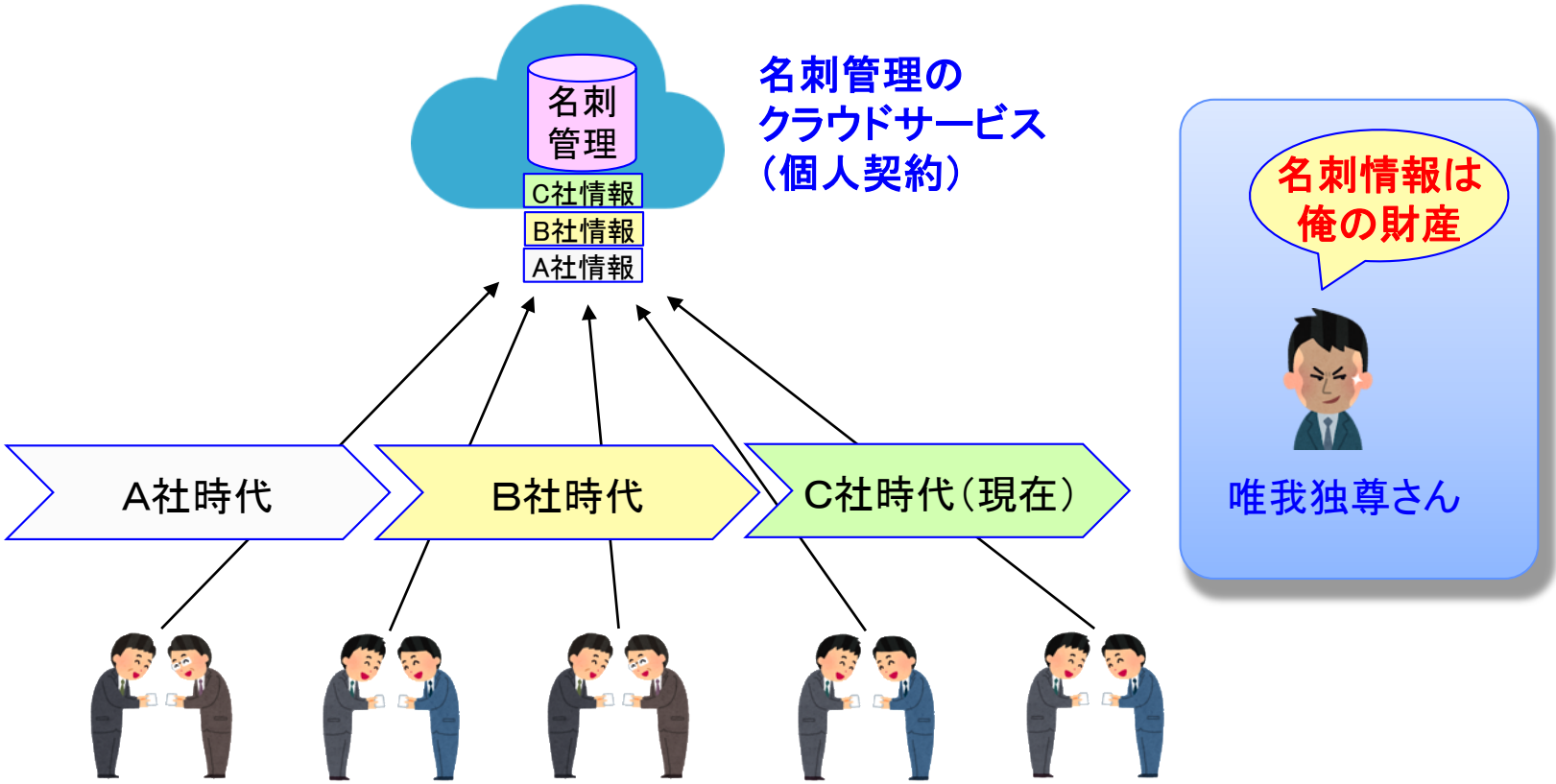
組織管理外

クラウドサービス（SaaS）としての名刺管理アプリの利用事例

事例B：サービス利用時における野良クラウド （カテゴリ4）

事例概要

・公私混同の事例として**個人として契約して使える名刺管理アプリを利用**し、
お客様や関連するベンダから**受領した名刺情報をクラウド上に管理＆活用**していた
・名刺サービスの利用は前職から実施しており、別会社に転職してもそのまま使い続けており前職の名刺情報も混在して保管されているという事例報告



事例B：サービス利用時における野良クラウド （カテゴリ4）

背景

個人で使えるAPの**導入が比較的安価**（名刺管理アプリ）に利用可能

・簡単に契約出来る
・安価（1日のタバコ代相当）

唯我独尊さん

問題点（発生要因）

①**名刺情報は**個人がもらったものなので**自分の財産**だから自由に使えるという認識誤り
②個人契約のクラウドサービスの検知が出来ない（**システムでチェック不可**）

・名刺情報は個人情報保護の対象となることの認識が無い
・個人契約＆私有PC/スマホでの利用だとシステム検知は不可

課題

①業務上入手した**名刺情報は会社に帰属**し、**個人情報**に該当するので適切な管理が必要だという認識を植え付ける

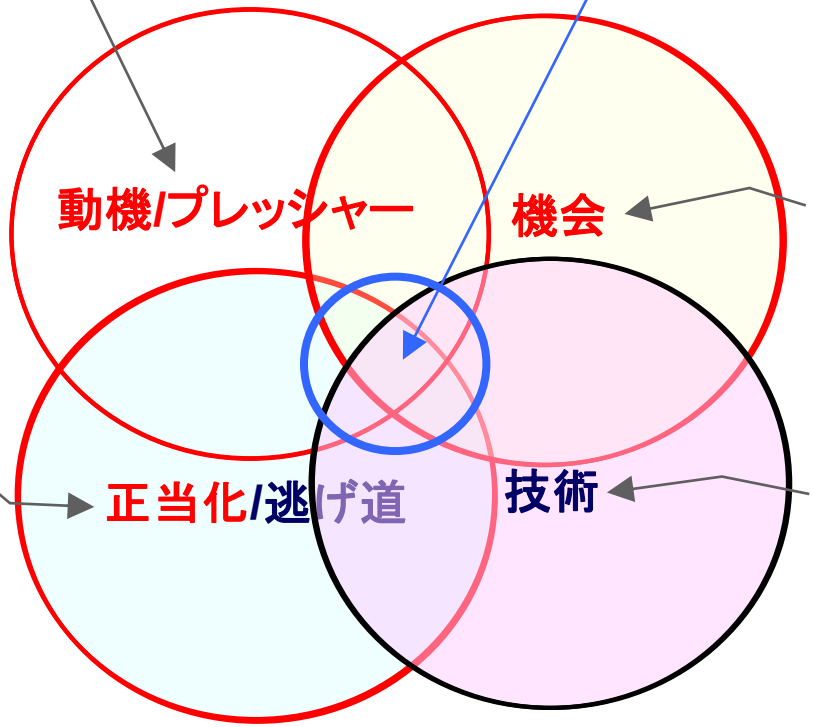
・保護対象となる情報と管理方法についての再認識
・名刺情報の管理を個人管理ではなく会社での一括管理の是非

②個人契約のクラウド利用の検知＆排除（**野良クラウド利用の禁止**）

・個人契約のクラウド利用の禁止ルールが明文化されていない
・オンラインでの検知方法が無い

要因分析のツール： インシデント（不正）発生のスクエア

動機がなければ考えない（不満、不安、金銭的悩み、欲望、利益（見返り）、など、動機となる原因を調査し、観察する）

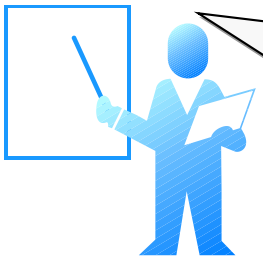


四要素が重なっている部分で問題が発生し易い。

機会がなければ実行できない（機会を与えない）

自己正当化と逃げ道がなければ実行し難い（監視、検知の仕組みと、記録、報告の徹底を行う）

技術がなければ実行できない（高度な技術で防御するか、管理者以外には変更できない仕組みとする）



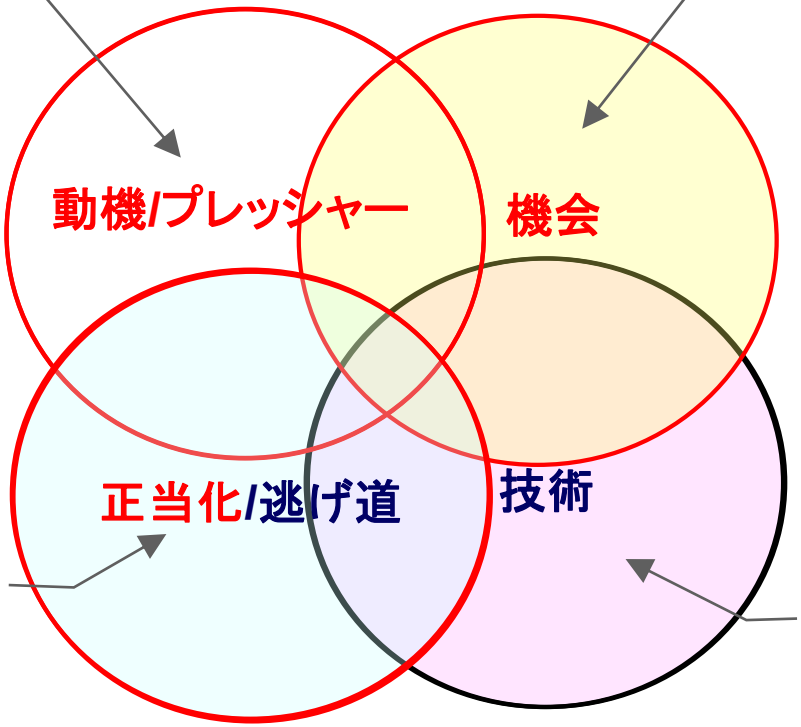
不正のトライアングル（赤〇の項目）は、米国の犯罪学者であるD.R.クレッシーが、人間（犯罪者）の心理面を研究して導き出した理論ですが、情報セキュリティの面からみると、トライアングル理論に、「技術」や「逃げ道」などを追加することで、より効果的にインシデントを防止できる可能性があります。

野良クラウド（名刺管理アプリ）を利用した要因は？

唯我独尊さんの深層心理

・簡単に契約可能
・**安価に利用可能**
・業務の効率化が図れる

・承認機能が働かない
（個人契約のクラウド）
・チェック機能が働かない
（**システム検知不可**）
・クレジット払いで簡単

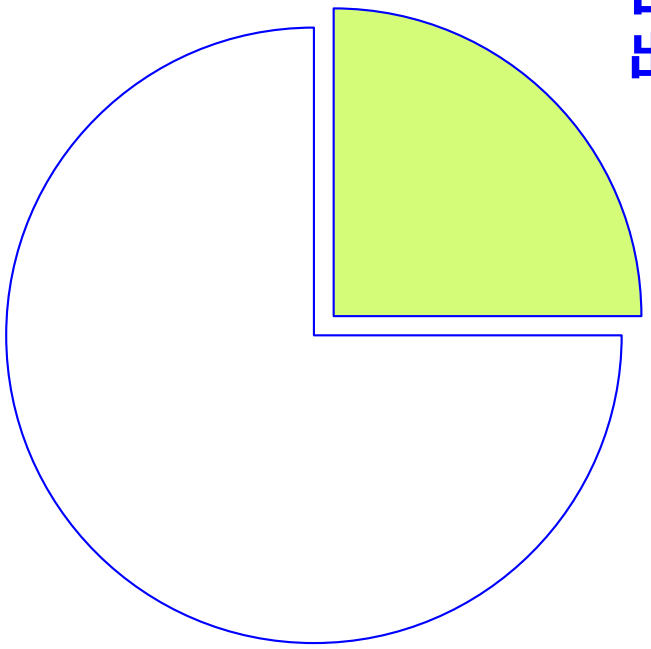


・**名刺情報は自分の情報**
（自分の人脈＆財産）
という誤認識
・**個人情報保護法の認識不足**
・自らDX化を実践
・**野良クラウド利用禁止**
ルールがない

・クラウドサービス
なので、技術がなく
てもすぐに利用可能

- **簡単、安価、便利**
- **業務効率化**
- **見つからない**

組織管理外サービス（特に野良クラウド）の利用の防止



目に見えないもの（システム検知が出来ない）を可視化するには？

◎ ルール可視化
＆ チェック

- クラウド利用のルールがない
- 野良クラウドの利用がリスクに繋がることの意識がない
- 管理運用プロセス（正規クラウドの登録＆利用）がない
- 組織管理外サービス（野良クラウド）利用時の罰則等が制定されていない
- 内部監査時のヒアリング項目に入っていない

事例 C

A.情報のシフト
（社内領域→社外領域）

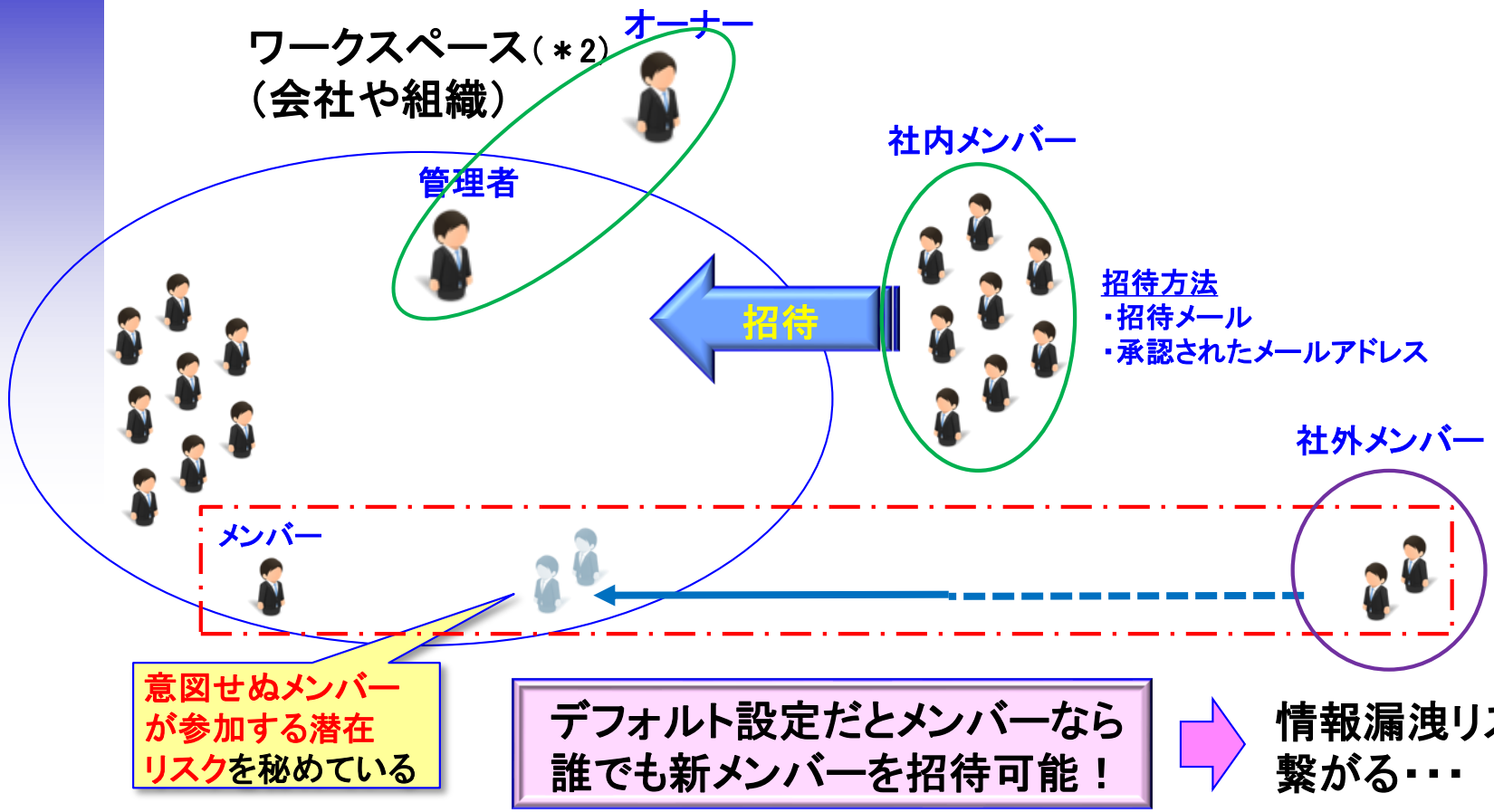
組織管理外の
サービス利用

**C.非正規の
使い方**

クラウドサービス利用時における課題の認識

NO	分類	発生事象	現状＆課題
C	非正規の使い方	承認範囲外での利用や誤用による情報漏洩やサービス停止リスク	組織として承認した範囲を逸脱することによる想定外のリスクが発生 事例紹介 →社内限定の空間に社外メンバーを招待 ・無関係なメンバー（客先/委託先）が招待され重要な機密情報が共有＆漏洩 ※：異動/退職後のアカウントの放置、権限付与の設定ミス、権限委譲による運用の乱用など （管理責任者の不在、管理の有名無実化） →私有PC/スマホなどの無断使用による情報漏洩 ・セキュリティ対策不備によるマルウェア感染 ・紛失時の事後対応遅れ →許可プロジェクト以外での利用拡大 ・禁止事項（個人情報などの保管）抵触による情報漏洩リスク（利用実態が把握出来ない、検知手段がない） →誤用によるサービス停止 ・間違ってサービス解約することでインスタンスが消滅し、復旧処理が出来ないなど（知識不足＆簡単にコンソールで処理が可能）

事例：グループウェア（＊1）を題材とした情報共有について



※：ワークスペースの オーナー と管理者だけに招待する権限を限定するにはオプション契約が必要

＊1：Slack、ZoHo、teams、LINEなどのクラウドサービス
＊2：グループウェアのワークスペースはプロジェクト全体で考えると会社や組織のような存在

グループウェア導入に関連するペルソナの心の声

経営層

・ISMS事務局員
・**規則　守**（45歳）

ビジネスのスピードアップを目的としたグループウェア導入を決定！

・お客様SI案件のPM
・**唯我独尊**（32歳）

グループウェアの適用範囲は社員に限定するというガイドライン制定

取り敢えず社内限定でPoCを実施し、全体像が見えてから適用範囲を拡大したい（半年～1年）

クラウド上のアクセス権管理や情報管理、利用の管理方法が見えない

→社内システムだと情シスがすべてを把握していたが、クラウドでは各々の部門で管理するため、管理がずさんになる可能性を秘めている
→どこにどのような情報を格納しているのか可視化が難しい
→私有PC/スマホ経由で情報漏洩の可能性がある

強い反発

導入目的はお題目なのか？
（社員だけでは効果が出ない！）

半年もPoCをしているとプロジェクトが終わってしまう！
浦島太郎か？

プロジェクトの推進は同一居室内で社員、派遣社員、請負社員一体となって行なっている。ビジネスのスピードを上げるために社員だけにグループウェアを導入しても導入効果が出ない！

悪魔の囁き

実質管理は部門なので、例外運用するか？

→ビジネス優先のためには手段を選ばない、ルールには例外規定がある！
社員以外がいても絶対にバレない
（プライベートチャネルはメンバー以外は存在もわからない）

グループウェアの適用範囲は社員に限定する背景

反発を受けてもグループウェアの適用範囲を社員に限定する理由

・クラウド上のアカウント管理やアクセス権管理が見えない！
・手作業による運用管理では限界がある！

SAML（Security Assertion Markup Language）を利用することで、人事システムと連動したAD連携で退職時には自動的にアカウントが利用出来ないようにしたい！

・クラウドのアカウント管理が社内で管理可能
・認証ログとの連携でクラウドサービスの利用者を管理可能
・私有PC/スマホでのアクセスが制限可能

制約事項

社内の認証と連動させて管理するためには社員限定とする必要がある

クラウドの認証にも社内と同じ認証の仕組みを！

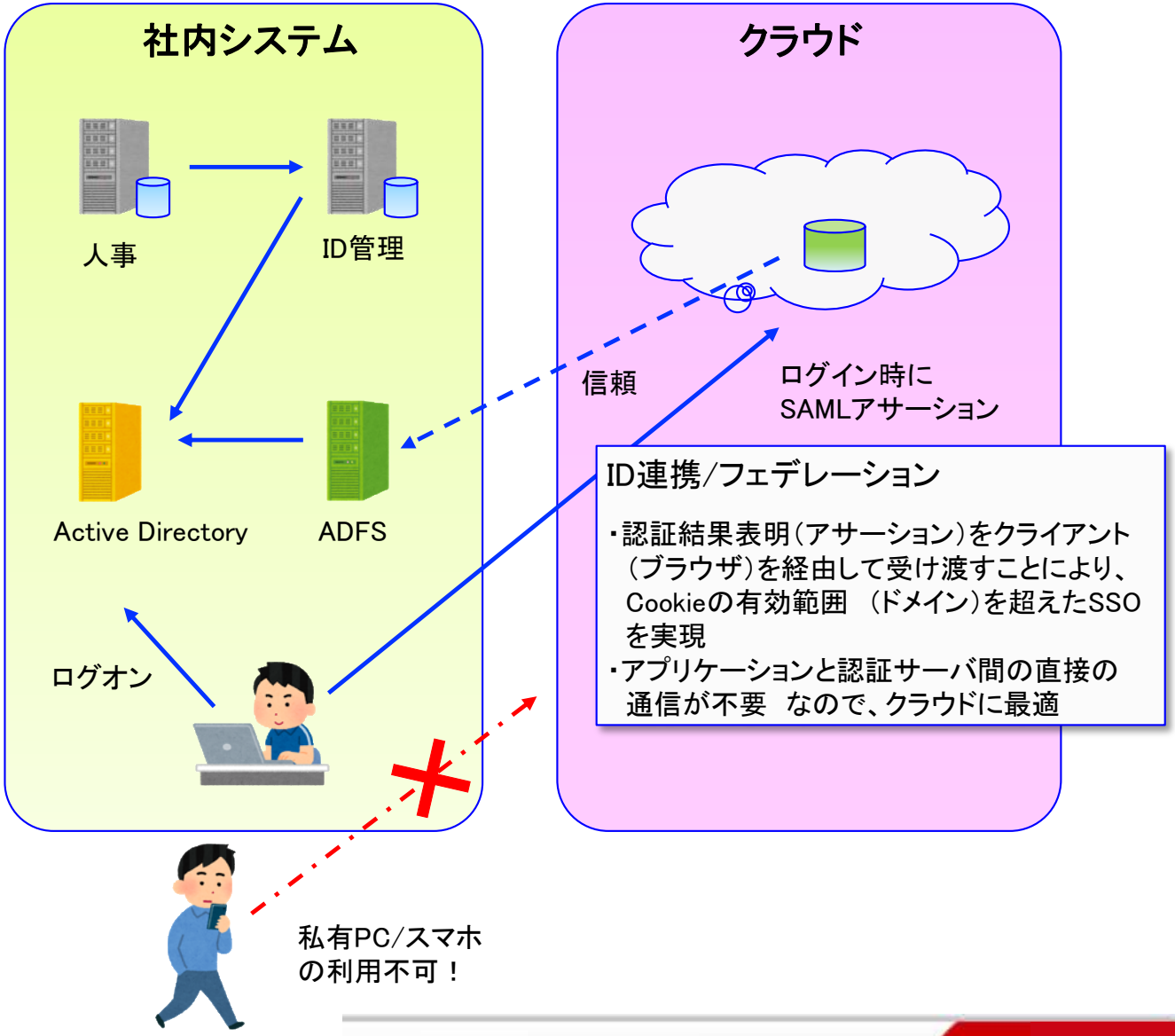
課題解決

・ISMS事務局員
・**規則　守**（45歳）

SAML導入

〇運用管理の負担軽減

- **異動/退職に連動した権限削除**
- **私有PC/スマホの利用制限**
- **社内と同じスキームで運用**

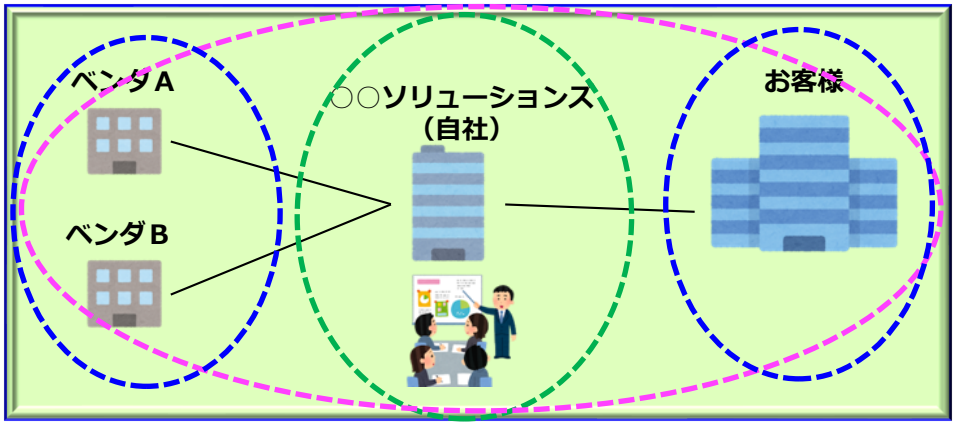


反論！　社員に限定した運用は意味が無い！！！

問題提起

ビジネス自体が自社だけに閉じてなりたっているのではなく、サプライチェーンによって成り立っているので、適用範囲を社員に制限することでワークスタイルの変革に足枷をかけることになってしまう！

・お客様SI案件のPM
・**唯我独尊**（32歳）

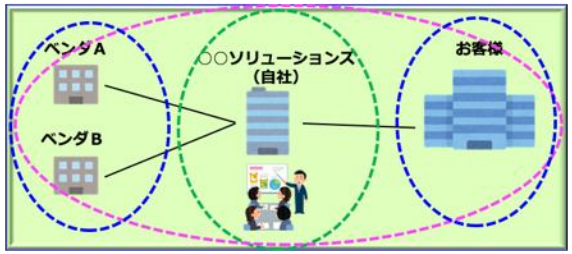


ガイドラインの範囲

サプライチェーンの枠組み

従来ベース（メールなど）の情報共有は疎結合状態となる！

ビジネスとセキュリティのバランスが必要！



ガイドラインの範囲

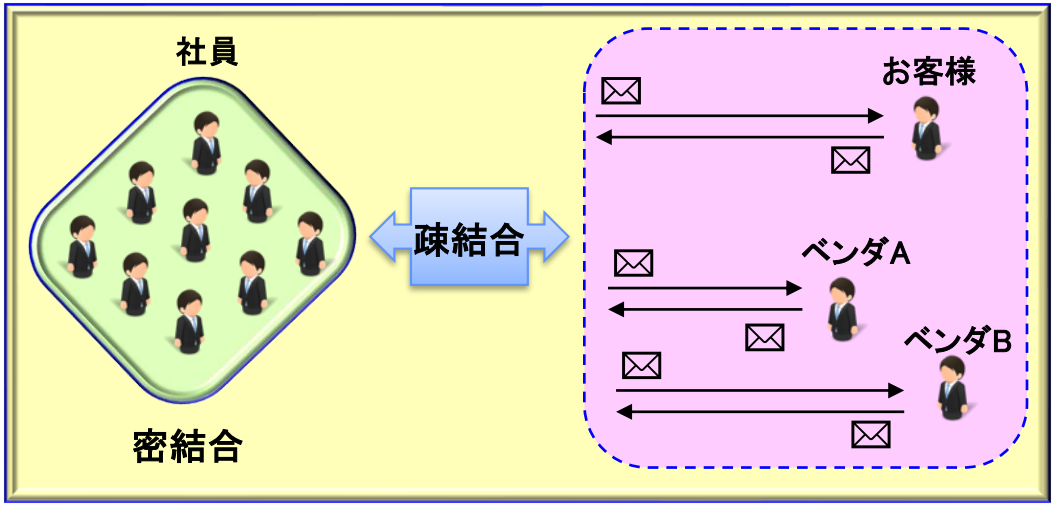
サプライチェーンの枠組み

従来ベース（メールなど）の情報共有は疎結合状態となる！

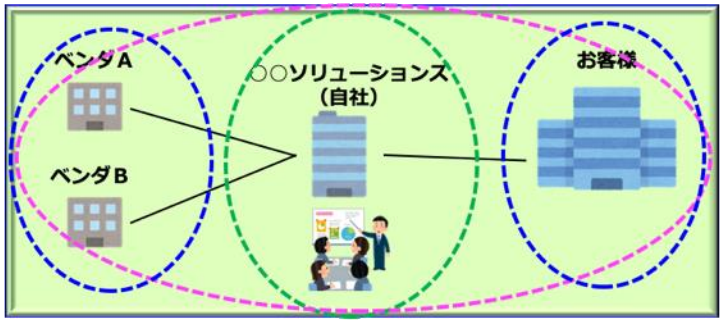
サプライチェーンの枠組み無しでのビジネスは想定出来ない

自社内のコミュニケーションの効率化を実施しても効果は期待薄！

ビジネスとセキュリティのバランスを考慮した導入の枠組みが必要



サプライチェーン枠組みにおける情報共有の在り方



ガイドラインの範囲

サプライチェーンの枠組み

グループウェアによる情報連携

ゲスト招待 ＋ SAML認証による厳密な管理 ＋ ゲスト招待

運用管理　システム管理　運用管理

PMによる人手管理

○対策事項

・SAML認証を導入で運用管理の負担を軽減
・適用範囲外のベンダ（請負先）やお客様へ導入はゲスト招待で対応

アクセス権管理については現場のPMにて実施することになるので、形骸化しない対応プロセスが必要！
また、リスクとして下記の対応の検討も必要

＜コンプライアンスの問題＞

対お客様：

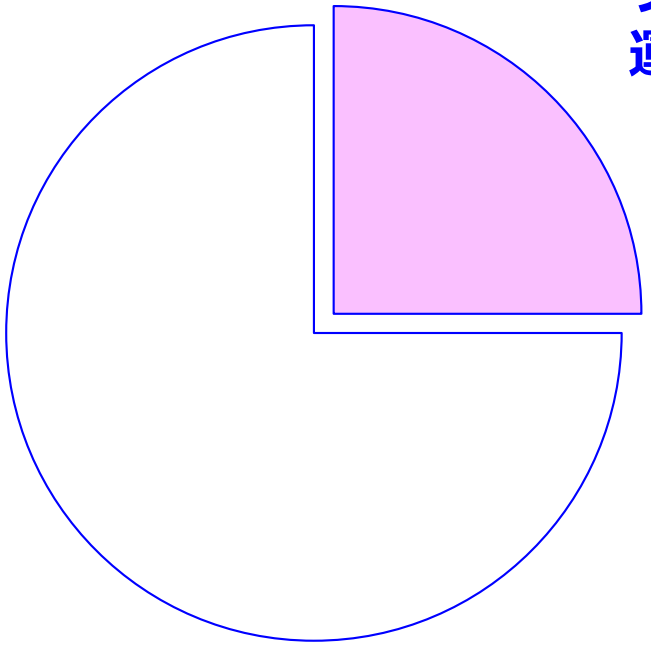
・仕様の確定後の追加要望の扱いの整理が難しい（単なる意見か、仕様変更の要望か？）

対ベンダ（請負先）：

・ベンダへの情報共有なのか、指示命令なのかが曖昧となる。現場の管理責任者以外への指示があれば命令系統違反（偽装請負など）へ結びつくリスクがある

事例Cから導かれる分析＆課題

非正規の使い方による承認範囲外での利用や誤用による情報漏洩やサービス停止リスクへの対応

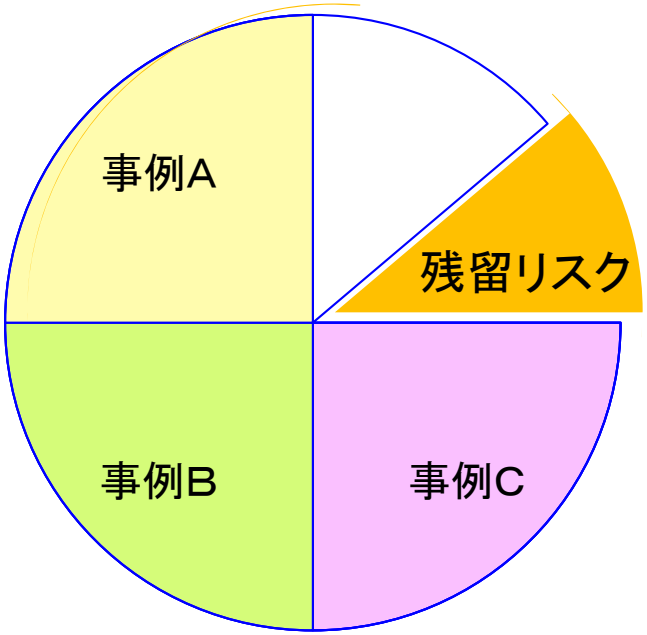


クラウドの特性を知らないと間違った運用で情報漏えいに繋がる！

◎ クラウド特有の管理要件 ＆ 管理プロセス

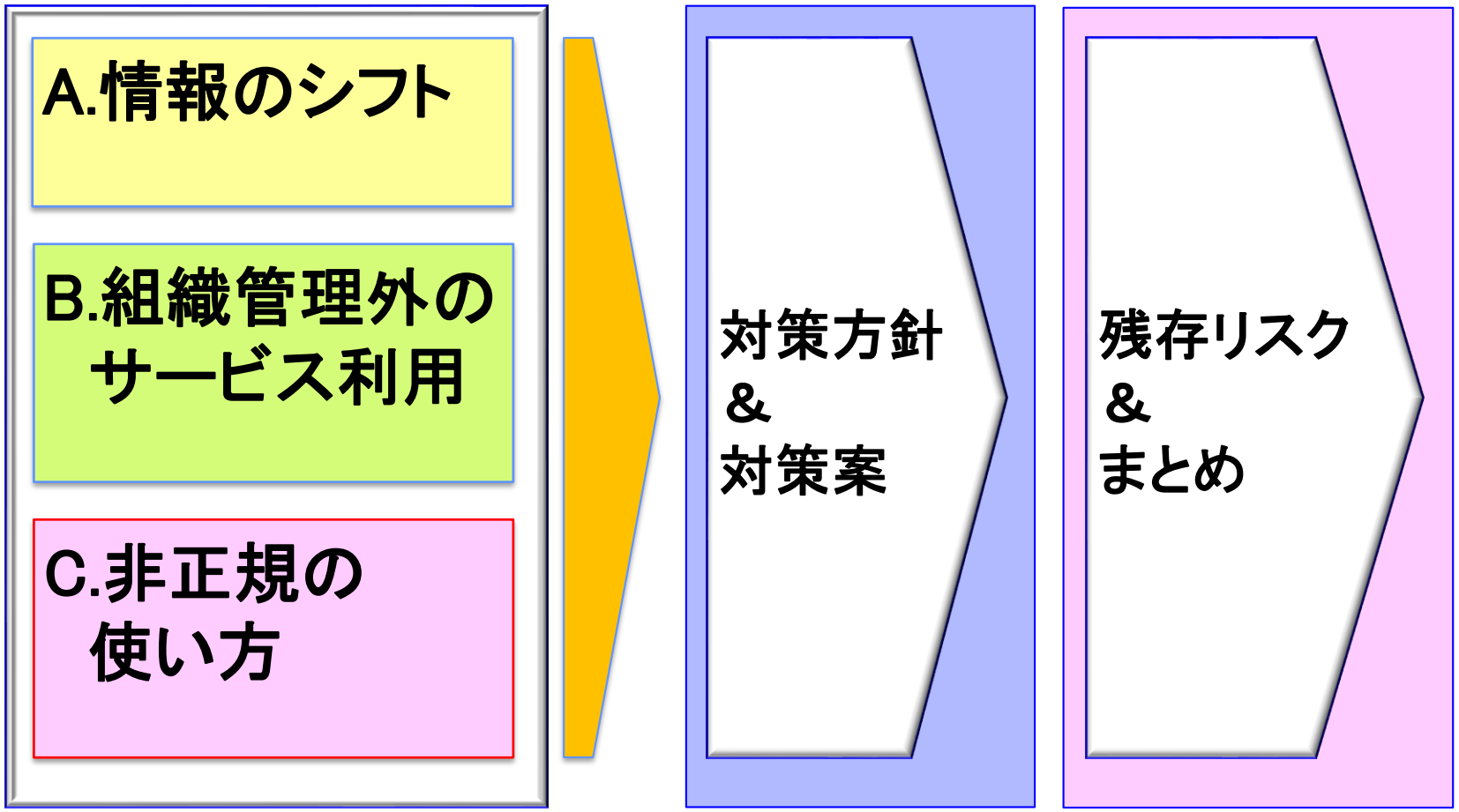
- 無関係なメンバー（客先/委託先）の招待による機密情報の漏洩
  ※：異動/退職後のアカウントの放置、権限付与の設定ミス、権限委譲による運用の乱用など（管理責任者の不在、管理の有名無実化）
- 私有PC/スマホの無断使用による情報漏洩
- 許可プロジェクト以外での範囲外利用
- 誤用によるサービス停止

まとめ



事例A～Cから導かれる
対策案と残留リスク

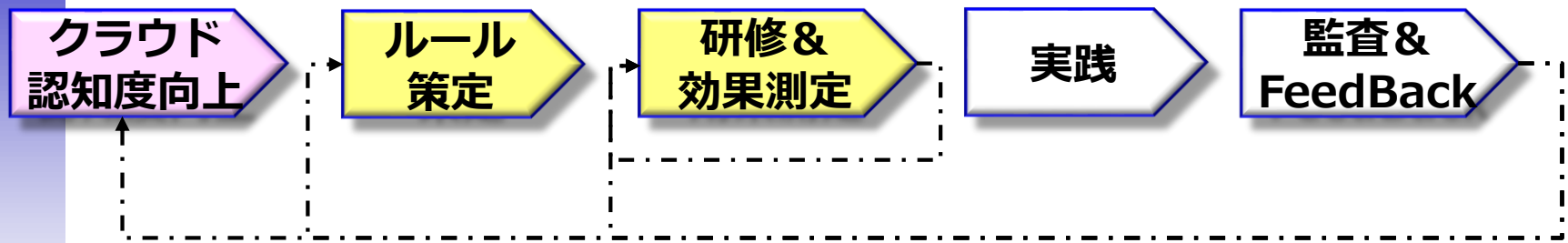
対応方針＆対策案



対応方針＆対策案

事例		対応方針	対策案
A	情報のシフト（社内→社外）による管理要件の変化	◎クラウド時代の情報管理 従来の管理方法では不十分！ クラウド特有の管理要件の設定が必要 （事例Ｃと連携）	・アクセス権管理の管理者明確化 （ワークスペース単位） ・管理者への意識付け＆リマインド （職務定義の明確化、有名無実化しない） ・クラウドサービスによって異なる仕様を意識 （管理方法やアクセス権限の利用者への移譲範囲）
B	組織管理外サービス（野良クラウド）の利用の防止	◎クラウド利用の基本ルール設定＆利用状況の可視化 野良クラウドの定義とリスクの認識 正規サービスの可視化＆一覧化	・クラウド利用の基本ルール（*1）の制定 *1:システム台帳に登録し、組織管理下 ・管理運用プロセスの策定（正規クラウドの登録＆利用について手続き）と利用状況の可視化 ・野良クラウド利用リスクの意識付け ・利用時罰則等の制定 ・内部監査時のヒアリングによるチェック
C	非正規の使い方による承認範囲外での利用や誤用による情報漏洩やサービス停止リスクへの対応	◎クラウド特有の管理要件の可視化＆意識付け クラウドの特性を知ることで間違った運用による情報漏えいリスクを防止	・無関係なメンバー（客先/委託先）の招待による機密情報の共有＆漏洩防止 ※：異動/退職後のアカウントの放置、権限付与の設定ミス、権限委譲による運用の乱用など →SAML認証の導入 ・私有PC/スマホの無断使用による情報漏洩防止 ・許可プロジェクト以外での利用禁止 ・誤用によるサービス停止

クラウド利用時のガバナンスの全体像



- クラウドとは？（一般常識）
- どういうものがクラウドか？（具体例）
- 主要リスクの認識

- 規定類の整備
- →システム管理台帳含む
- ルールブックの策定（申請/承認）（アクセス権管理）
- 罰則規定

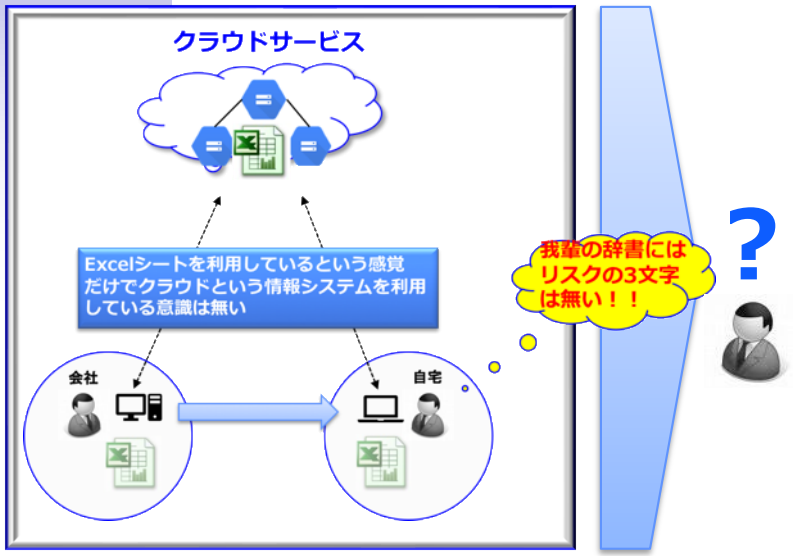
- 社内ルールの理解
- インシデント発生時のビジネスインパクトの理解
- リスクアセスメントの実践研修
- ルール逸脱時の罰則理解
- 効果測定結果に基づく再研修

- 利用申請&承認
- リスクアセスメント実施
- システム管理台帳登録
- アクセス権管理

- 日々の運用チェック（自治点検&アンケート）
- 内部監査による重点チェック（サンプリング）
- →野良クラウドの検出含む
- GAP分析&ルール見直し等のFeedBack

従業員の意識向上（知る→理解→実行）

クラウド利用時における一般ユーザの認識レベルは低い！



正しい行動を促すためには？

知る → 理解 → 実行

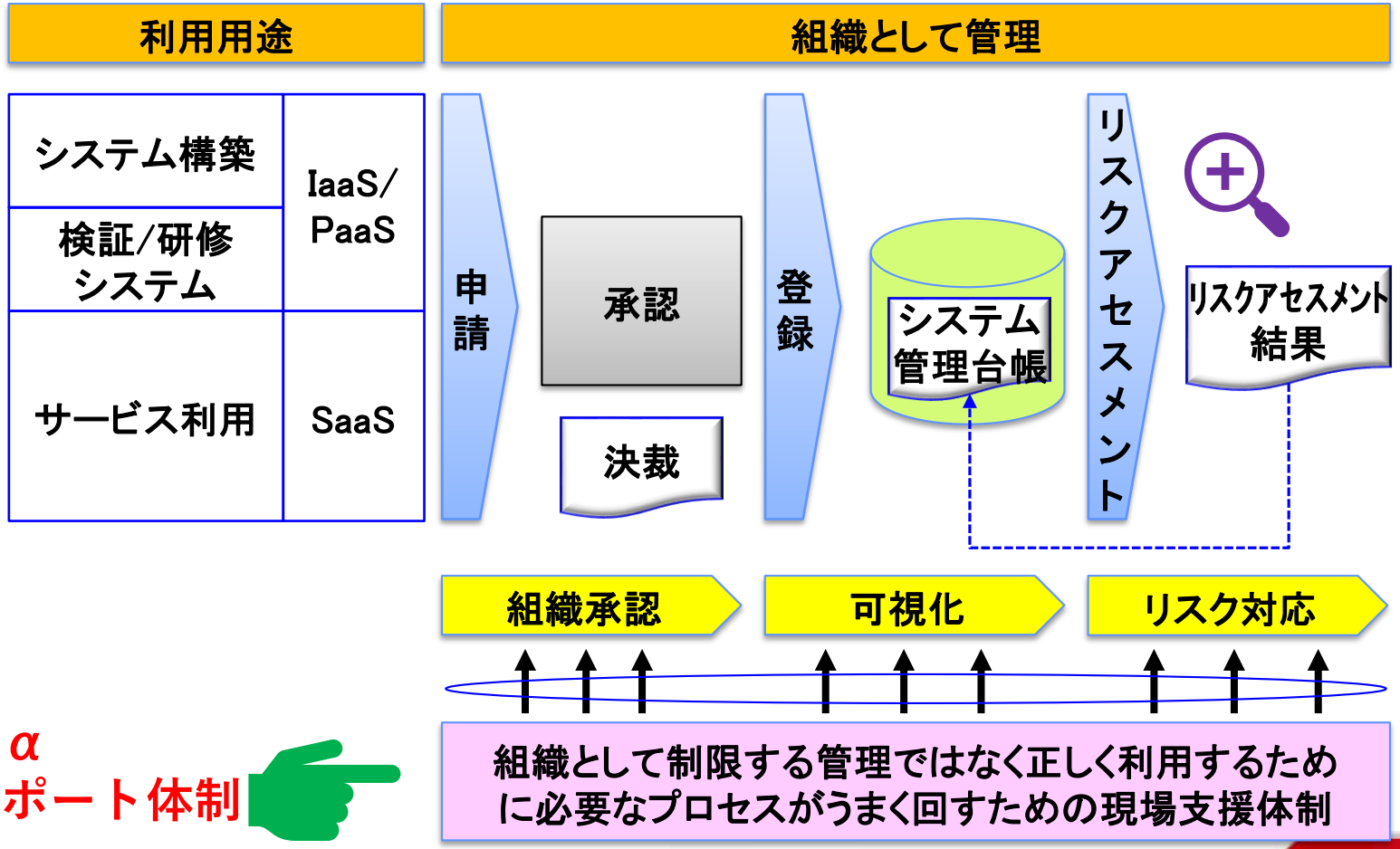
認識	遵守
・クラウドサービスとは？ ・具体例としてクラウドサービスの識別が出来る ・クラウドの主要リスクを認識 ・インシデント発生時のビジネスインパクトを理解 ・ルール（申請～承認、許可/禁止行為）を認識 ・罰則規定を理解	・申請～承認 ・許可範囲での利用 ・リスクアセスメントの実施 ・クラウド利用の登録＆管理

啓蒙活動

・ルールブックの策定＆周知
・研修＆理解度測定＆ﾌｨｰﾄﾞﾊﾞｯｸ

組織として管理（ルール化＆可視化）

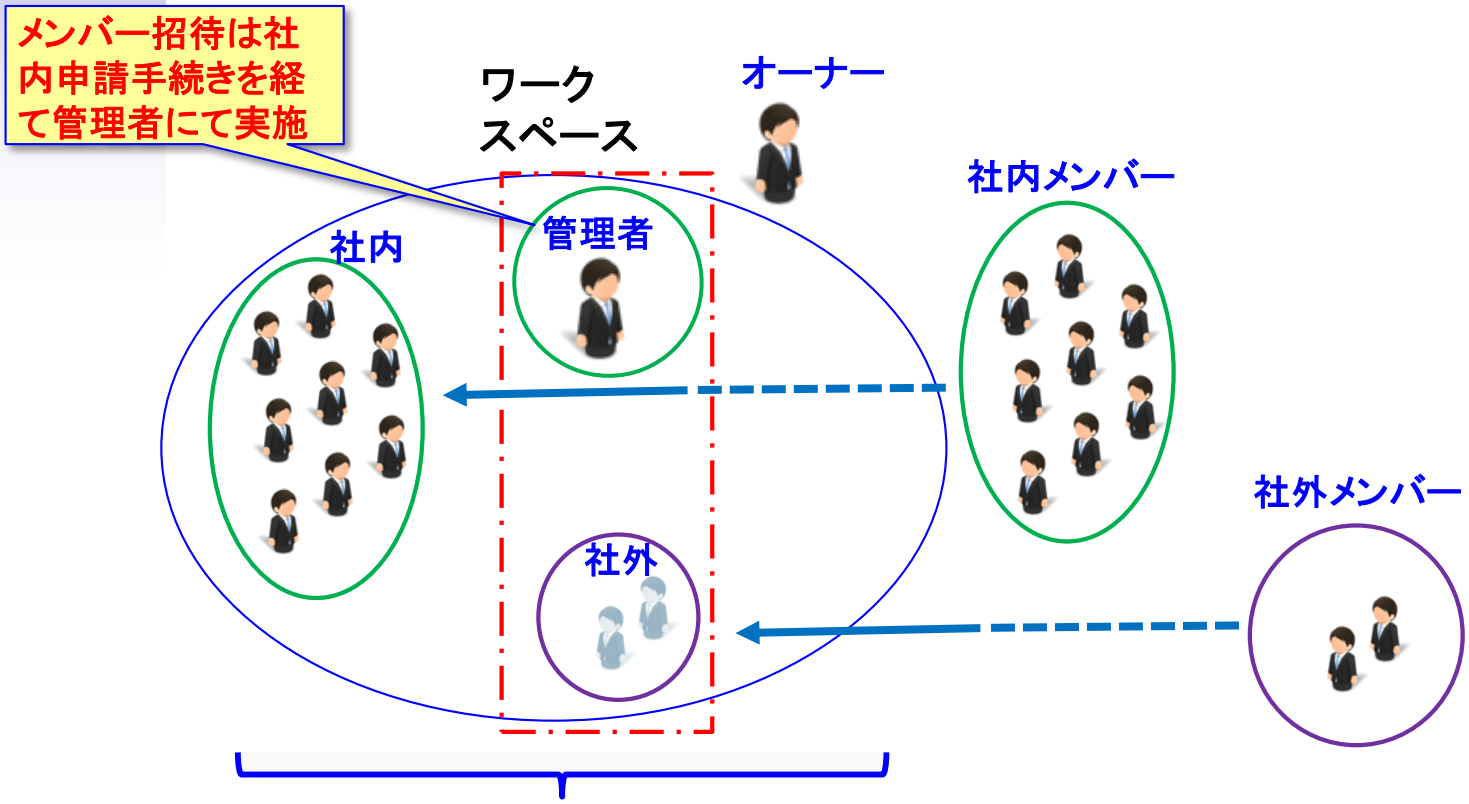
- クラウド利用の可視化（システム台帳に登録。サービス利用も）
- 申請～承認プロセス　（申請帳票、決裁）
- リスクアセスメントの実施（リスクの可視化）



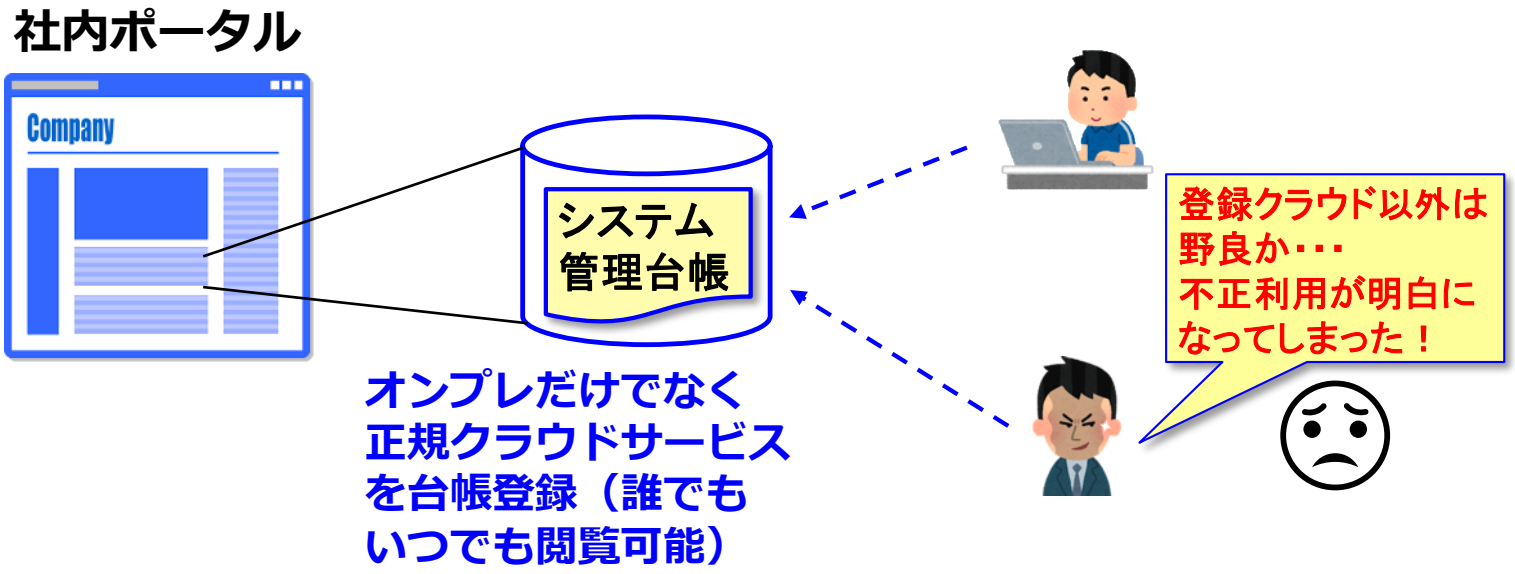
事例A　クラウド時代のアクセス権管理

◎ クラウド時代の情報管理 ＆ 管理プロセス

・アクセス権の管理者の明確化
・管理者への意識付け＆リマインド
・アカウントの定期的な棚卸し



事例A/B　システム管理台帳への登録＆公開義務



- システム管理台帳へIaas/PaaS/SaaS含めてすべて登録を実施
  （システム名、用途、管理者名を明記）
  →管理者への意識付け
- 必ず、社内ポータルなどに公開することで正規クラウドを認識
  →それ以外は野良クラウドという識別を明確化
- 定期的な棚卸しによる最新化
- 内部監査時のインプット情報としても活用

事例B　可視化手法（その1）

内部監査のヒアリングによる可視化

内部監査の重点確認項目にクラウドの項目を追加し、ヒアリングを実施する！！！

資産台帳に記載されている情報資産〇〇をどう管理されていますか？

△△クラウドを利用して効率的に管理しています

情報資産台帳

システム管理台帳

△△クラウドですね。了解しました。
ただ、△△クラウドはシステム台帳には記載されていないようですが・・・

オンサイトツアーで必ず実務者にヒアリングを行う！

事例B/C　可視化手法（その2）

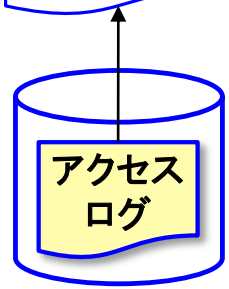
クラウドへのアクセスログによる可視化

不適切事例の検知＆抑止

このクラウドへアクセスしたというログ
を元にヒアリング
（アップロード/ダウンロード履歴含む）

クラウドへの
アクセスログ

△△クラウドへのアクセスがありますが、
このクラウドサービスは許可されていない
はずですが・・・



お客様指定で△△クラウドを利用していました。
お客様指定なので、社内ルールの適用外だと
判断していました・・・

お客様指定です。
何か異論がありますか！

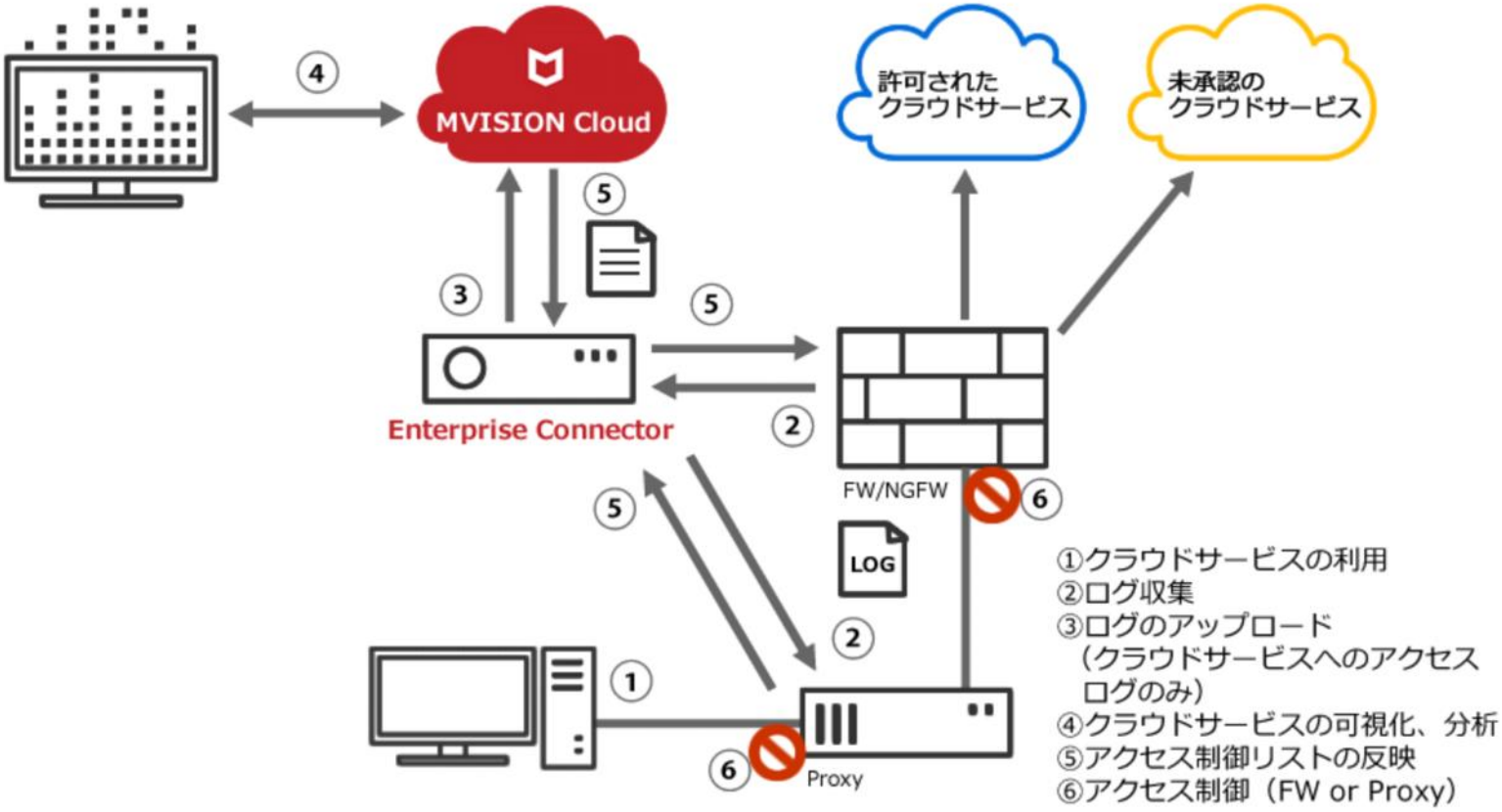
野良クラウドを単純に
排除するのではなく、
野良を受け入れること
で野生化させない取り
組みも必要！

監視の体制が出来ることで、
不適切事例を検知し、抑止に
繋げることができる

事例B/C　可視化手法（その3）

CASBソリューションによる可視化

・クラウドサービスの利用状況を可視化し、詳細に分析された27,000以上のクラウドサービス情報をもとにリスク判定
・暗号化やアクセス制御、振る舞いによる脅威検知機能



https://www.techmatrix.co.jp/product/mvision-cloud/overview.html

全体総括

最後のまとめ・・・

・クラウドの光と陰を意識する！（リスク認識）

・正しく使う！（誤るとインシデントに繋がる）

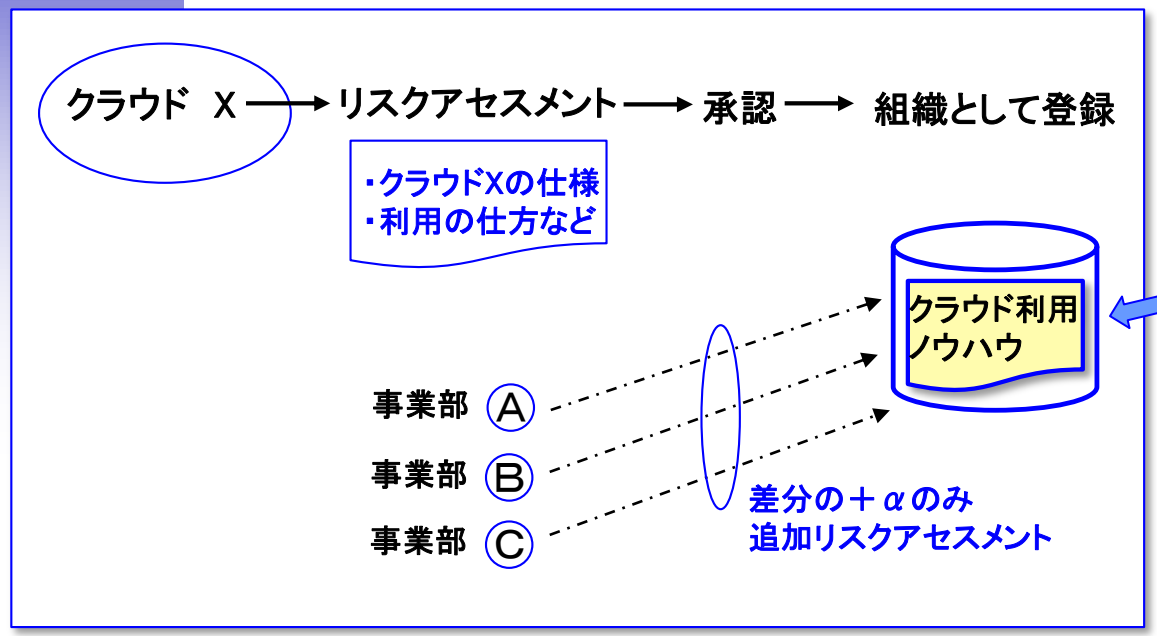
・システムで制限出来ない範囲がある・・・

・運用でカバーすることも重要
→システム＋運用のコラボレーション

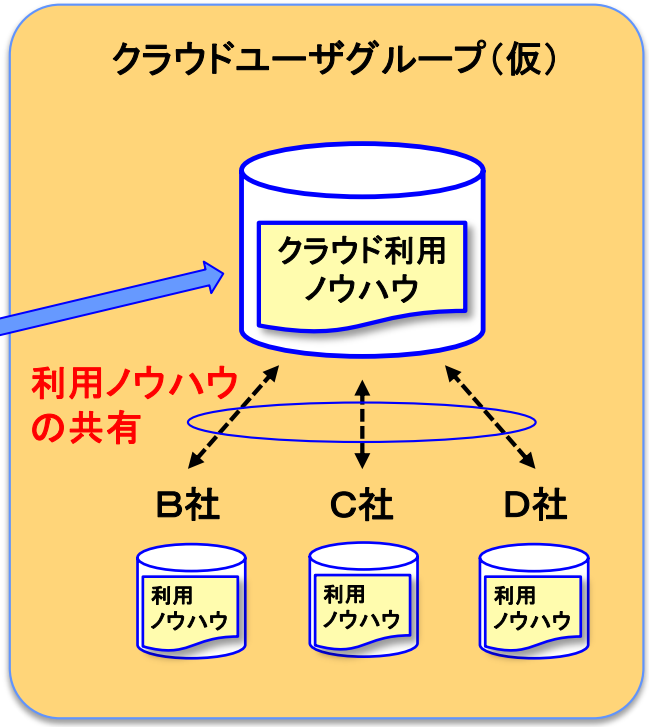
・野良クラウドの保護
→　野良クラウドを単純に制限するだけでなく、積極的に保護（正規クラウド化の承認やリスクアセスメントの支援）を実施

安心・安全なクラウドを遅滞なく使う！・・・理想

○○ソリューションズ株式会社



コミュニティなどによる情報共有



クラウドサービスを使いたい時に速やかにかつ安全に使う

- クラウドの仕様＆利用についてリスクアセスメントを実施
- 代表的なクラウドサービスなどは組織として事前に検証＆使い方のガイドラインを作成
- 利用ノウハウやリスクアセスメント結果は情報共有＆活用

○利用ノウハウの事例

- クラウド固有の特性
- 利用上の注意事項や共通マニュアル
- 運用のTIPS
  アクセス権管理、利用ログの活用など・・・

最後に活動の紹介（インプリ研）

皆さんも是非ご参加ください

〇毎月最終木曜日に定例開催（18:00～21:00）
〇前半テーマ1、後半テーマ2を集中討議
〇研究会のテーマだけでなく、各社の疑問や悩みも解決
　（コンサル目線ではなく、実践経験に基づく回答・・・）
〇会員でなくともオブザーバー制度でお試し参加可能

参加のご連絡はJNSA事務局まで・・・

インプリメンテーション研究会（討議模様）

ご清聴ありがとうございました。

本日のセミナーでは最新の環境変化に伴うISMSの実装検討（クラウドファースト時代のリスクマネジメントの事例研究）を題材に企業を取り巻くリスクに対してISMS＋αでどのように可視化＆対応すべきかについてご紹介させて頂きました。

今回ご紹介した内容は一つの事例にすぎませんが、今後皆さまの職場へ持ち帰って検討頂ければ幸いです。

ルンダーレ宮殿の中庭