テーマ

ISMS規格要求事項から紐解く 最新のビジネス環境リスク

（サイバー攻撃、クラウド利用への対応方法についての考察）

日本ISMSユーザグループ
インプリメンテーション研究会

2018年12月 7日

主査　魚脇　雅晴

インプリメンテーション研究会メンバー

インプリメンテーション研究会　メンバー		
No.	会社名	氏名
1	ISO/IEC JTC1/SC27/WG1	山崎　哲
2	NTTコムソリューションズ株式会社	魚脇　雅晴
3	NTTコムソリューションズ株式会社	原　路子
4	NTTコムソリューションズ株式会社	広田 正毅
5	NTTコムソリューションズ株式会社	梅　文夫
6	NTTコムソリューションズ株式会社	中谷　勝彦
7	NTTコムソリューションズ株式会社	徳永　安芸
8	株式会社NTTデータ	和田　義毅
9	NTTデータ先端技術株式会社	小澤　隆一
10	ＫＤＤＩ株式会社	橋本　秀行
11	株式会社日立製作所	相羽　律子
12	富士通株式会社	増田　浩次
13	富士通株式会社	阿部　正峰
14	リコージャパン株式会社	羽田　卓郎
15	リコージャパン株式会社	小梁　康志
16	リコージャパン株式会社	今井 岳彦
17	株式会社インターネットイニシアティブ	松原　勝美
18	NTTコミュニケーションズ株式会社	桜井　秀紀
19	株式会社NTTファシリティーズ エンジニアリング	帯刀　静夫
20	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
21	NECソリューションイノベータ株式会社	尾崎 幸彦
22	NECソリューションイノベータ株式会社	大熊 信也
23	NECソリューションイノベータ株式会社	森 親章
24	NECソリューションイノベータ株式会社	大平　泰寛
25	アイレット株式会社	中村　昌登
26	個人	間形　文彦
27	個人	大竹　秀昇
28	個人	小野　等
29	個人	岡野　裕樹
30	個人	奥山　浩伸
31	個人	冨田　吉弘
32	個人	葛西　章広
33	個人	宮本　豊
34	個人	秋山　健一

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 （新規格の要求条件に準拠） ■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 （サイバー攻撃、クラウド利用への対応方法についての考察） ■働き方改革における情報セキュリティ**	

テーマの背景と概要

○テーマ背景

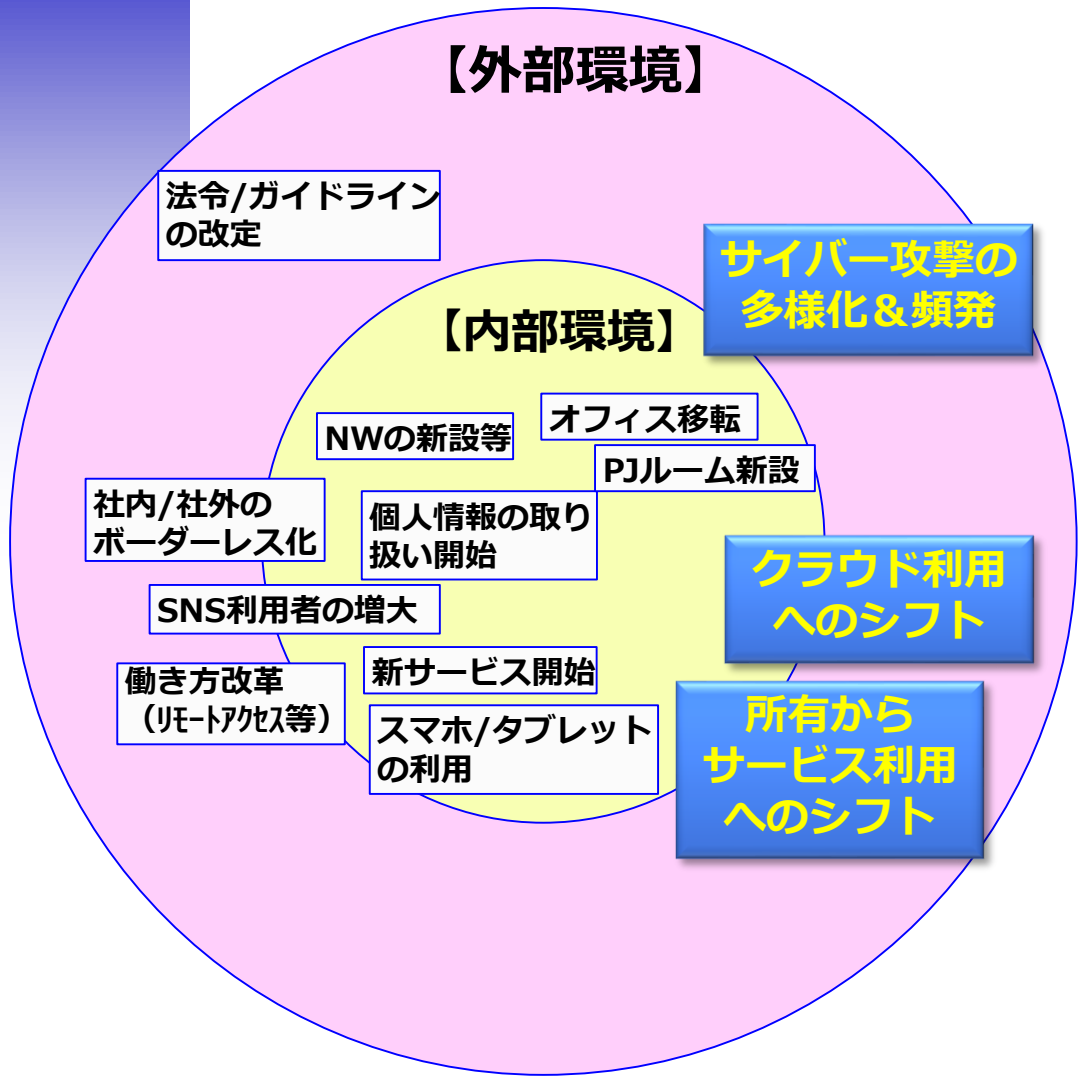
・企業を取り巻くビジネス環境のさまざまな変化
・新たなリスク（サイバー攻撃、クラウド利用）への対応
・従来のISMSの規格の枠組みでは対応が難しい状況

○テーマ概要

従来のISMSの規格の枠組みだけでは対応が難しい最新のビジネス環境リスク（サイバー攻撃、クラウド利用）に対して、組織的な対応を可能とするためアプローチについて提案する。

・組織的な対応に必要なフレームワークの整理
・各組織で構築済みのISMSの枠組みに加えて必要となる＋α（補足事項）を整理することで必要機能を可視化

企業を取り巻く環境の変化（外部/内部）



	リスク対応イベント（例）
1	オフィス新設/移転/廃止
2	PJルーム新設/移転/廃止
3	他ネットワークとの接続
4	新サービス･システムの導入/廃止
5	取扱う情報の変化
6	社内システム開発
7	外部サービスの利用（ASP、クラウド等）
8	リモートアクセスポイントの接続
9	検証ネットワークのウイルス対策等のセキュリティ対応
10	サイバーセキュリティ攻撃対応（随時）
11	法令/ガイドライン等の改定
12	人の意識の低下 SNSへの投稿、野良クラウド利用
n	・・・

ISMS事務局の悩み・・・

クラウド抜きではビジネスが
語れない、始まらない・・・
どのようにリスク対応すれば
良いのだろうか？

サイバー攻撃の対応として
CSIRT体制の構築と言われても
スキルも無い、投資の余裕も無い！

事例研究（Part1）

サイバー攻撃の
リスク対応

ISMS事務局の悩み・・・（サイバー攻撃対応）

ISMSは導入しているが、
サイバー対応するには
CSIRT体制の構築？

ISMSは構築運用しているが・・・

CSIRT体制の構築？

人／物／金はない！

ISMSの運用も兼務・・・

サイバー関連スキルの人材はいない！

ネット接続なしでは仕事にならない・・・

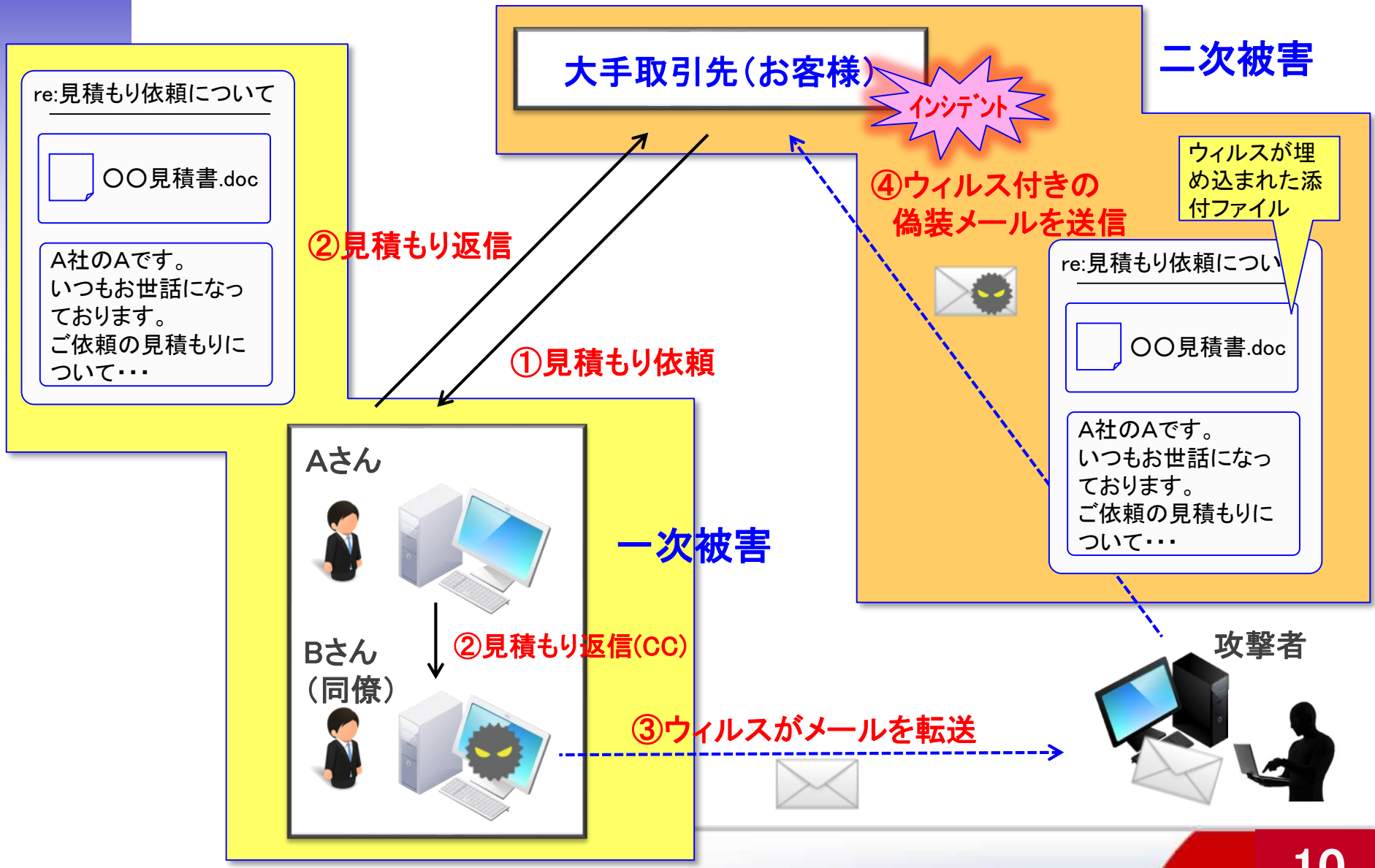
中小企業でもサイバー攻撃の対象・・・

課題設定とGoalイメージ（サイバー攻撃）

課題設定	テーマ終了時のGoalイメージ
・標的型攻撃メール等のサイバー攻撃の脅威 ・大企業で実装されつつあるCSIRT機能の実装は中小企業では難しい ・サイバー攻撃への対応を諦めることも出来ない！（サプライチェーンの枠組みや社会的道義）	**CSIRT体制構築が困難な企業向け簡易版実装の提言** （ISMSの実装にサイバー攻撃対応をアドオン）
参考事例： 被害者のはずが加害者に	
・中小企業でも実装可能なCSIRT機能を可視化 ・基本的なCSIRT機能の実装について現実解の模索	・現状のISMSの枠組みに＋αで実装 ・基本的なCSIRT機能の可視化 ・CSIRT機能を実装する上での課題整理（体制＆スキルセット）

参考事例：被害者のはずが加害者に（他社への影響）

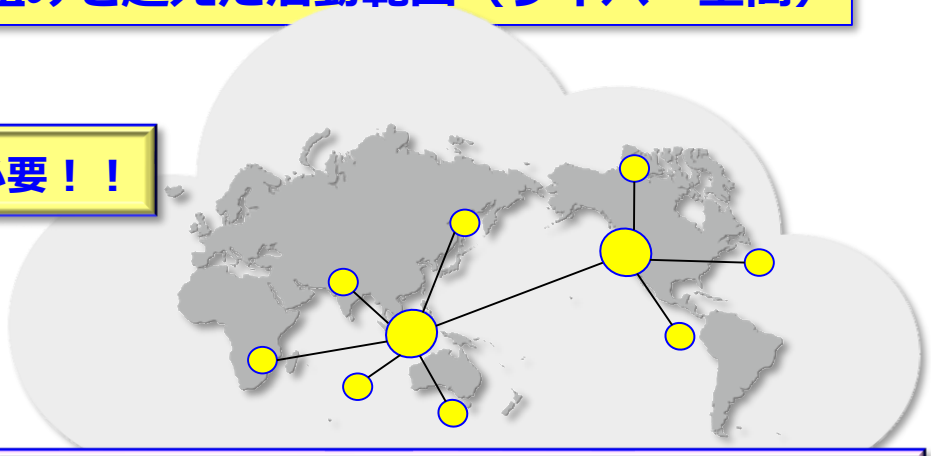
間接的に加害者となり、得意先に大きなインパクトを与える！



ISMSの活動範囲とサイバー空間について

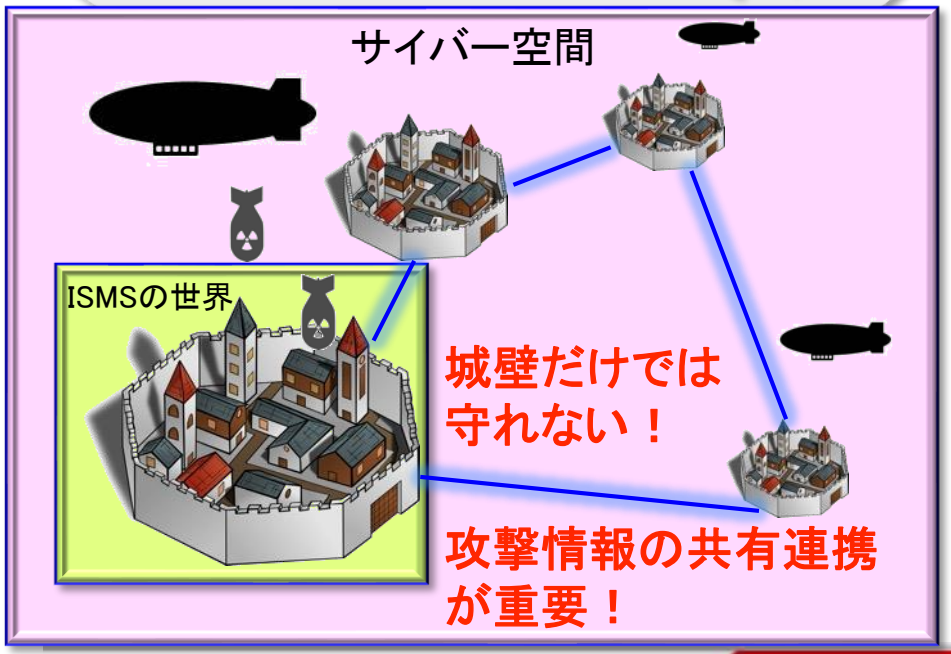
・ISMSは認証組織を中心とした活動範囲
・サイバー攻撃対応は組織の枠組みを超えた活動範囲（サイバー空間）

両者の違いを意識したリスク対応が必要！！



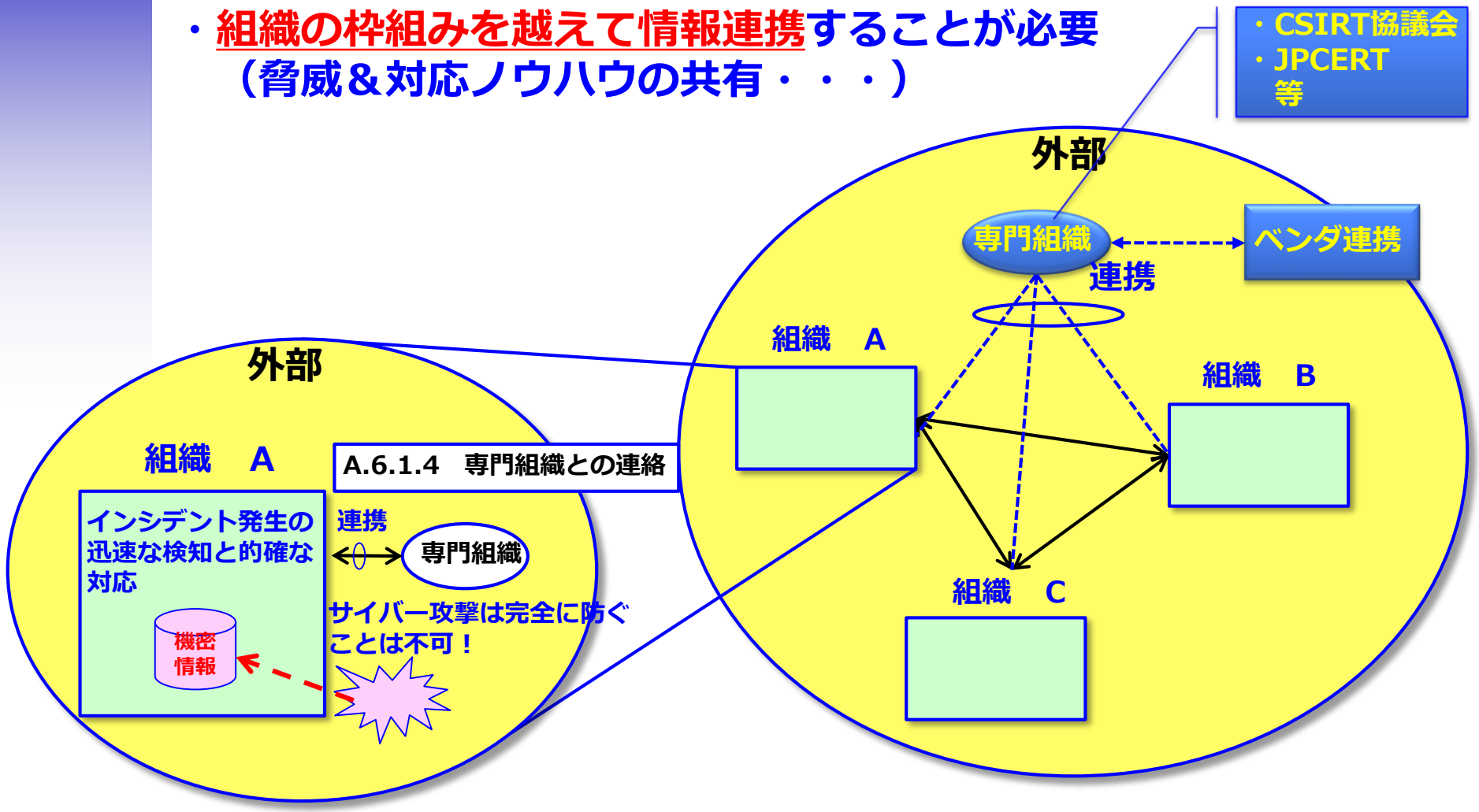
城壁の中だけを
守る世界

対比



他組織との攻撃情報や攻撃対応情報の共有

・サイバー空間に境界線は無い！
・組織の枠組みを越えて情報連携することが必要
（脅威＆対応ノウハウの共有・・・）



・自組織内だけでなく他組織との攻撃情報や攻撃対応情報の共有
（脆弱性情報の入手＆対応プロセス）

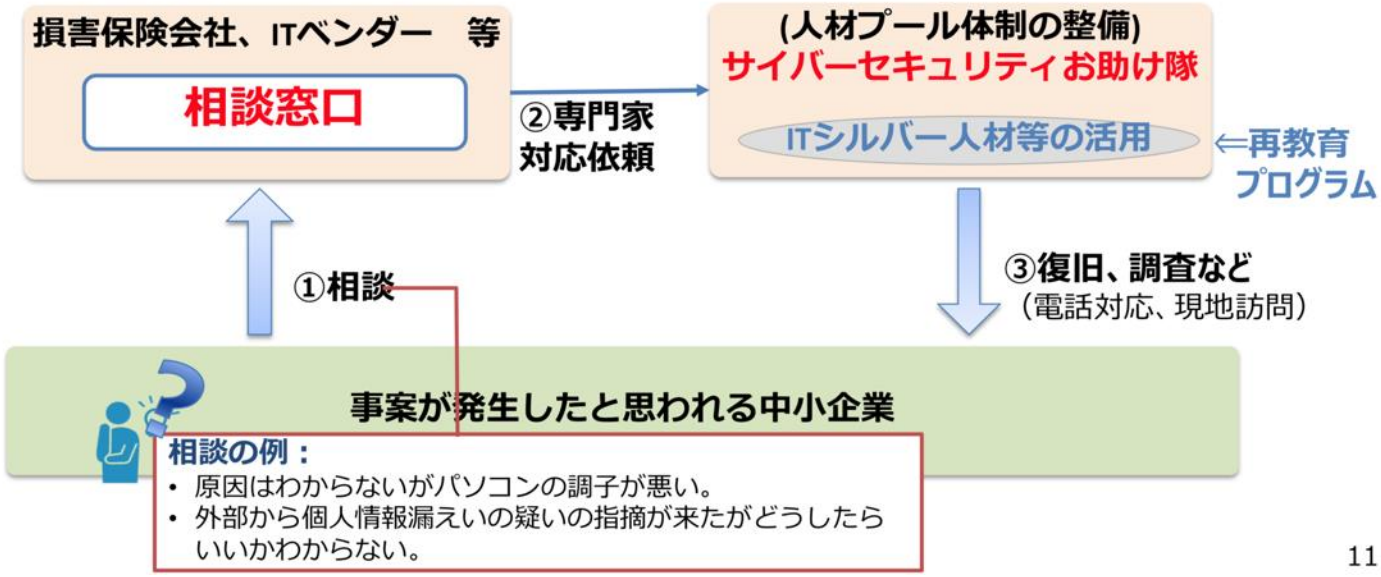
参考： 外部との連携先　『サイバーセキュリティお助け隊』

○産業サイバーセキュリティ強化へ向けた アクションプラン（経済産業省）

②中小企業向け：
サイバー保険等と連携して中小企業を支援する『サイバーセキュリティお助け隊』の創設

- 24時間相談窓口などの体制を持つ損保会社等と連携して、中小企業のサイバーセキュリティに関するトラブル対応を支援する『**サイバーセキュリティお助け隊**』を**創設**。
- ITに従事してきたシルバー人材の再教育などを通じて人的リソースを確保。

サイバーセキュリティ保険等と連携した『サイバーセキュリティお助け隊』のイメージ

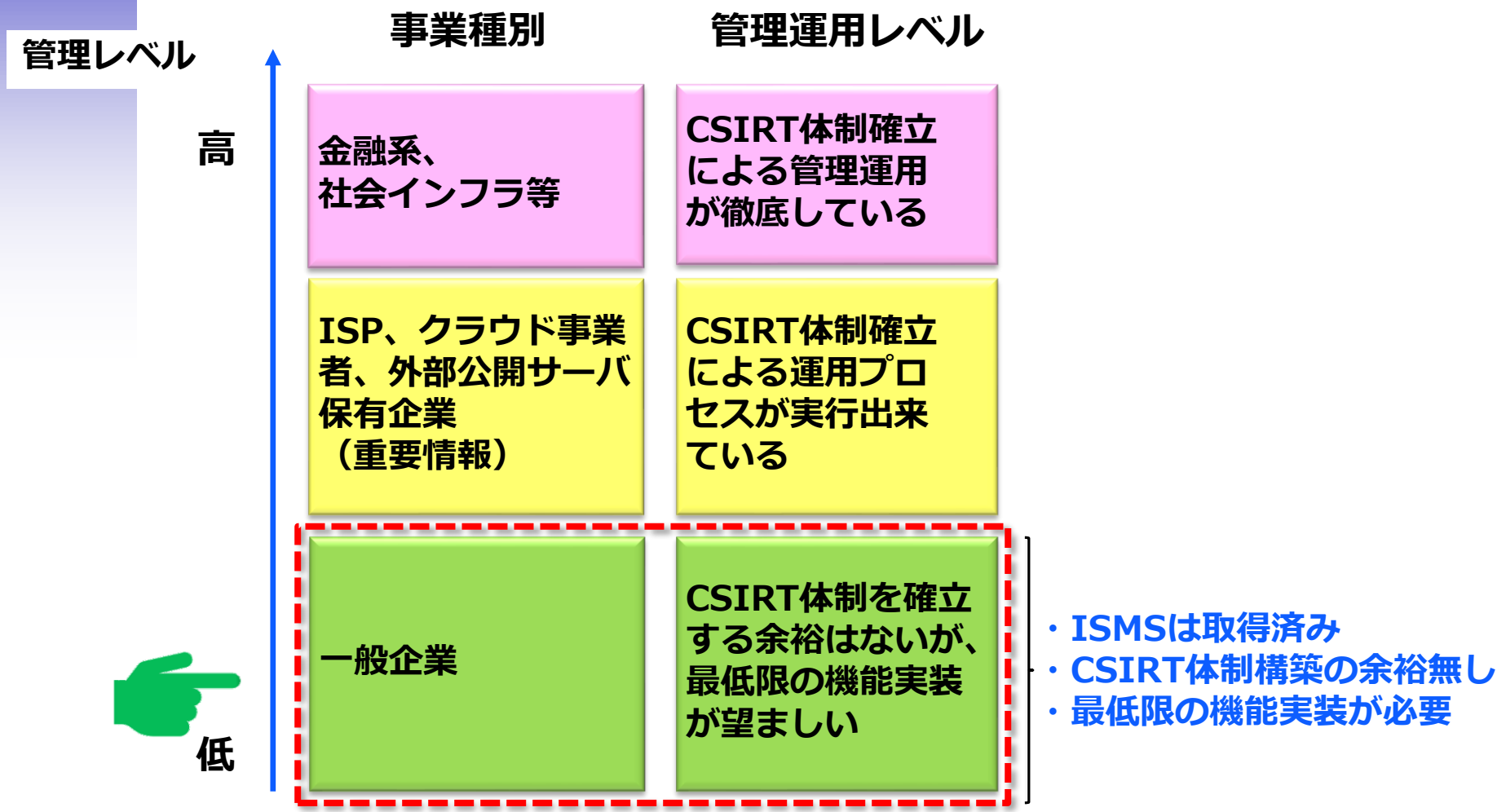


11

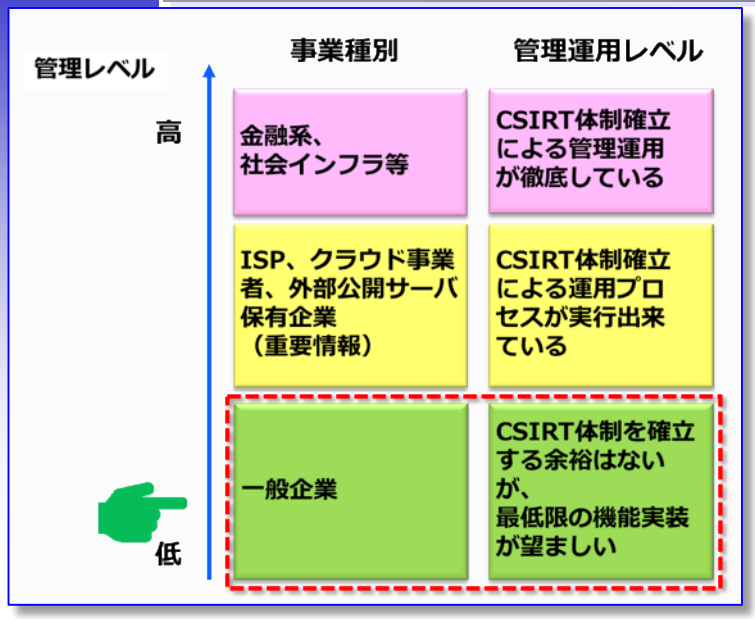
http://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/pdf/002_03_00.pdf

事業種別毎のサイバー攻撃対応の要求レベル

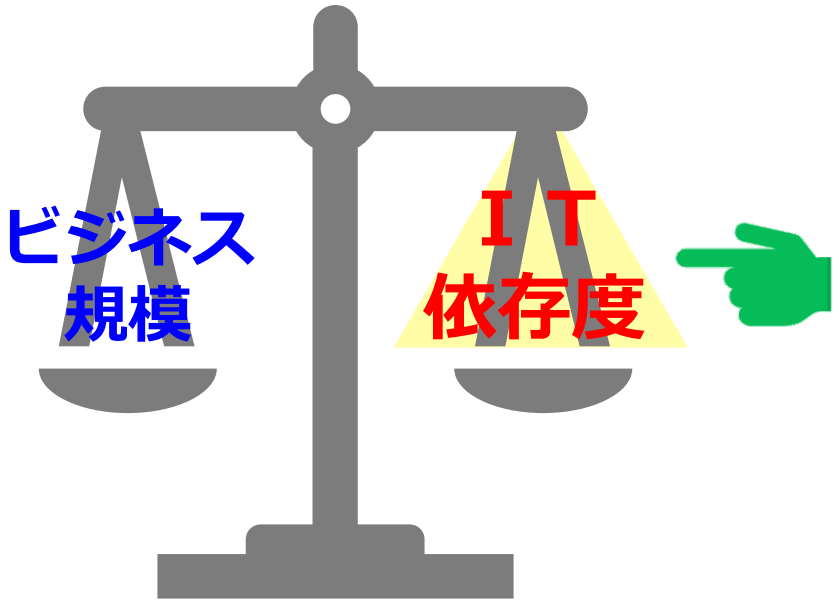
：今回の想定スコープ（絞り込み）



事業規模だけではないサイバー対応の要求レベル



ビジネス規模だけでなく
ＩＴ依存度も加味！！



小さな会社にCSIRTを構築する余裕はない！！

○CSIRTに必要な人数は？（CSIRT協議会アンケート）

設置時　5名未満37%　5～10名未満46%　10～20名未満15%　20名以上2%

活動後　5名未満11%　5～10名未満37%　10～20名未満37%　20名以上15%

○CSIRT機能の実装に必要な要員とスキルは？

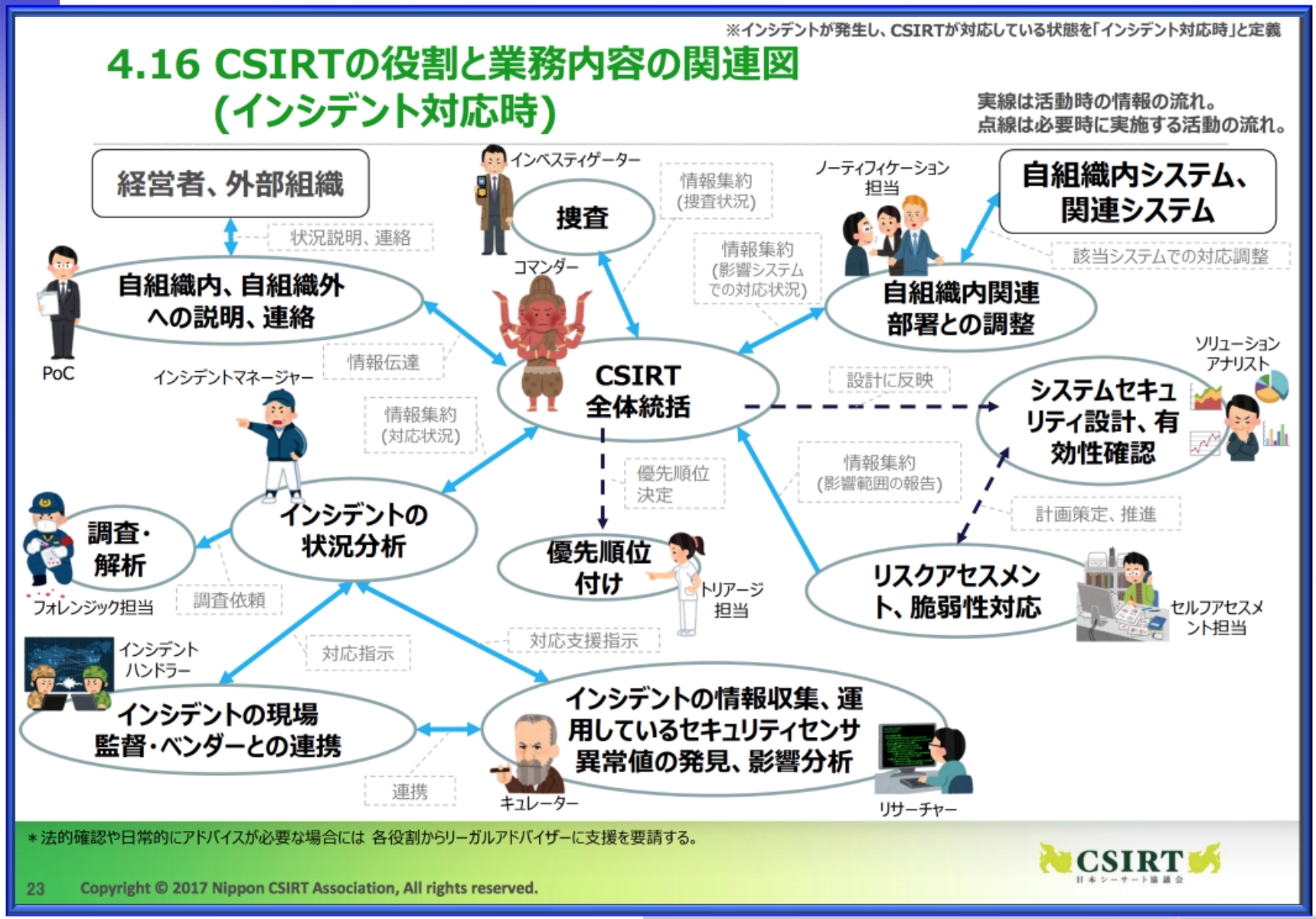
・高度なスキルを要求
　（次ページ参照：CSIRTの役割と業務内容の関連図）

・企業の業種、業態、ビジネスの要求事項に応じて様々なCSIRT体制

・会社規模の小さい組織はCSIRT体制を構築するのが困難

引用　JPNIC https://www.nic.ad.jp/ja/newsletter/No65/0800.html

参考：CSIRTの役割と業務内容の関連図（CSIRT協議会）



引用：CSIRT協議会資料　CSIRT人材の定義と確保http://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf

CSIRT機能の大分類

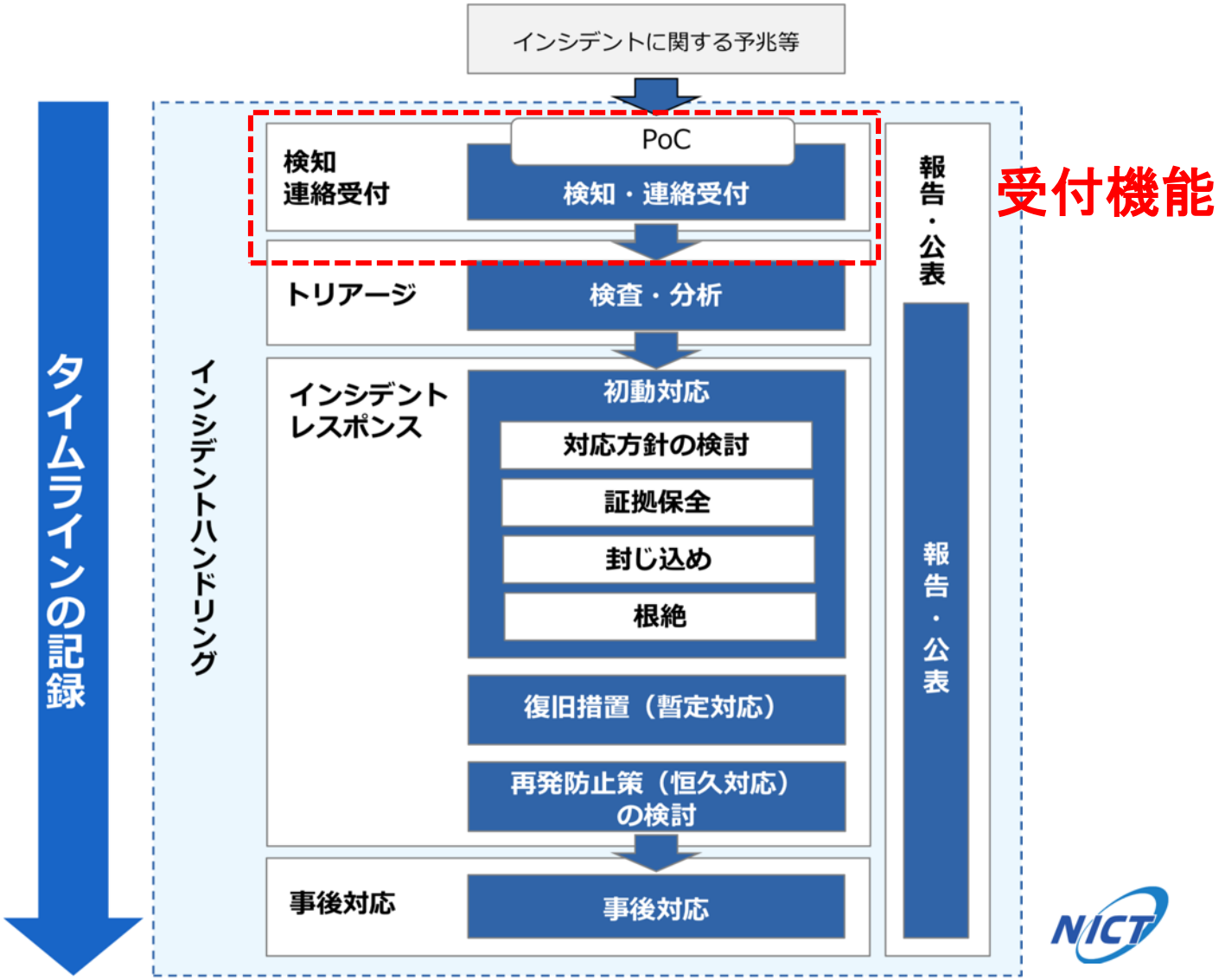
○CSIRT機能概要

★最初の一歩！

CSIRT機能	機能概要
受付機能（Point of Contact）	外部連携窓口（公開された窓口）、内部窓口 ・情報収集やインシデント発生後の対処や調査 ・脆弱性やインシデント情報を発見した時の窓口
技術的対応	外部から受け取った脆弱性情報などを技術的な視点で脅威を分析し伝達することや、調整活動、対外的な協力推進 （技術力＋コミュニケーション能力）
組織横断調整機能	・各部署との調整機能（インシデント発生時の公式見解や報道発表調整やセキュリティ戦略策定や教育） ・経営陣と現場との橋渡し機能
予防保全とインシデントレスポンス	・被害の未然防止のための脆弱性や攻撃情報の収集分析と早期検知 ・被害極小化のための迅速な対応と技術支援

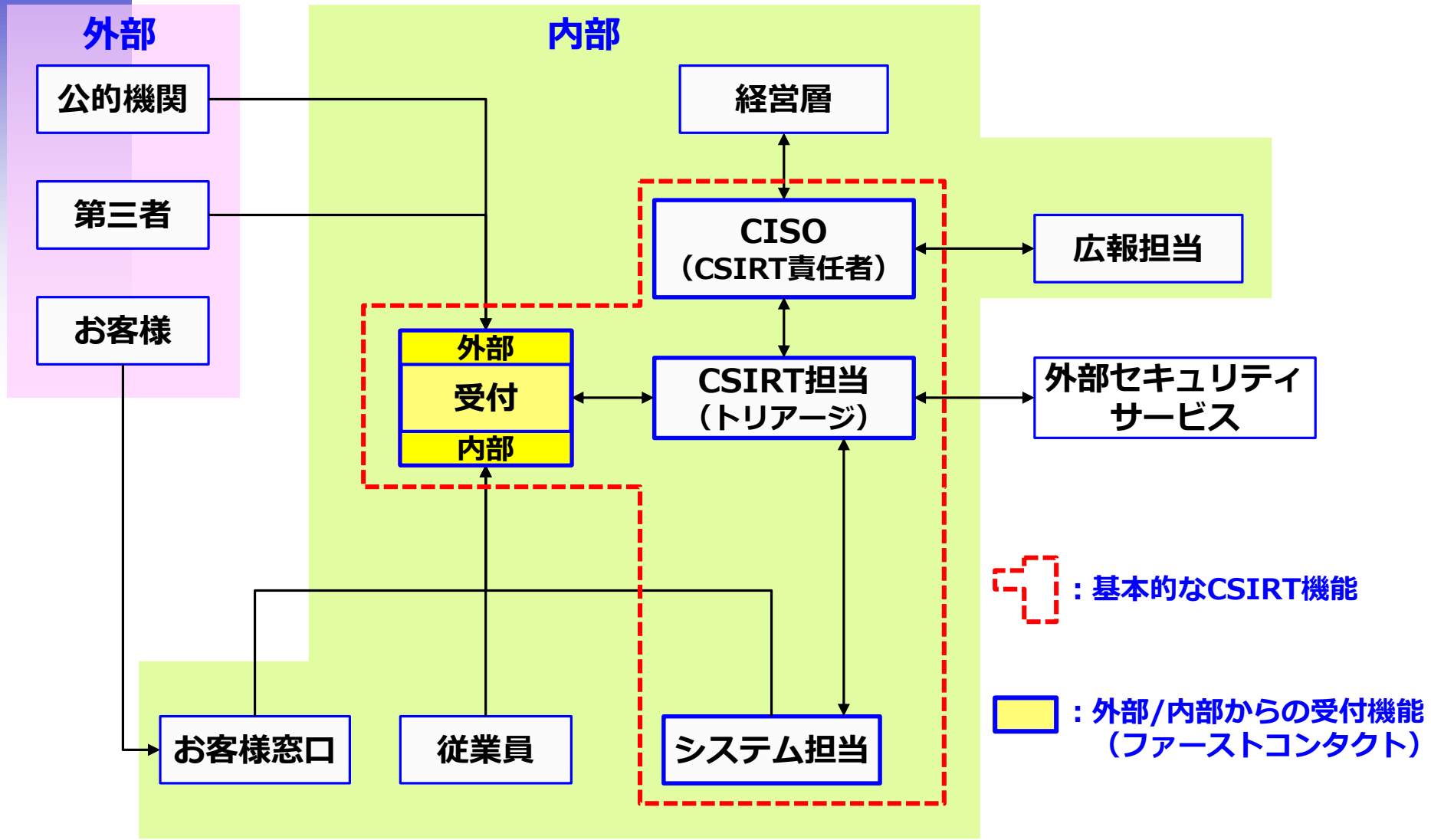
引用　JPNIC https://www.nic.ad.jp/ja/newsletter/No65/0800.html

参考：インシデントハンドリングの流れにおける受付機能



引用：実践的サイバー防御演習 「CYDER」紹介資料
https://cyder.nict.go.jp/files/CYDER-introduction_201807.pdf#search=%27nict+cyder%27

組織内の基本的なCSIRT機能



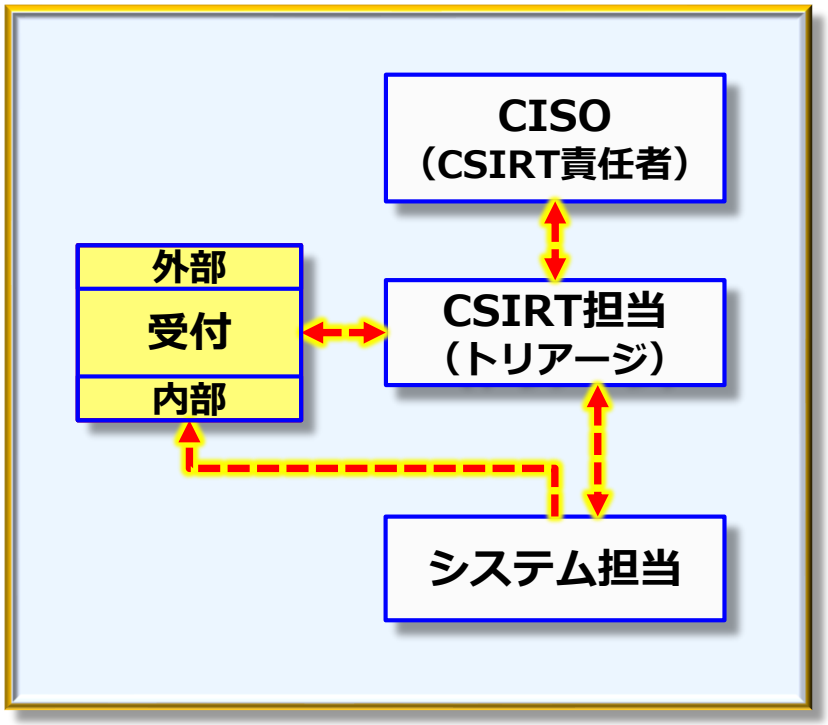
Coffee Break

ちいさな組織のメリット・・・

CSIRT体制を整備するには大きな組織の方が有利・・・

BUT

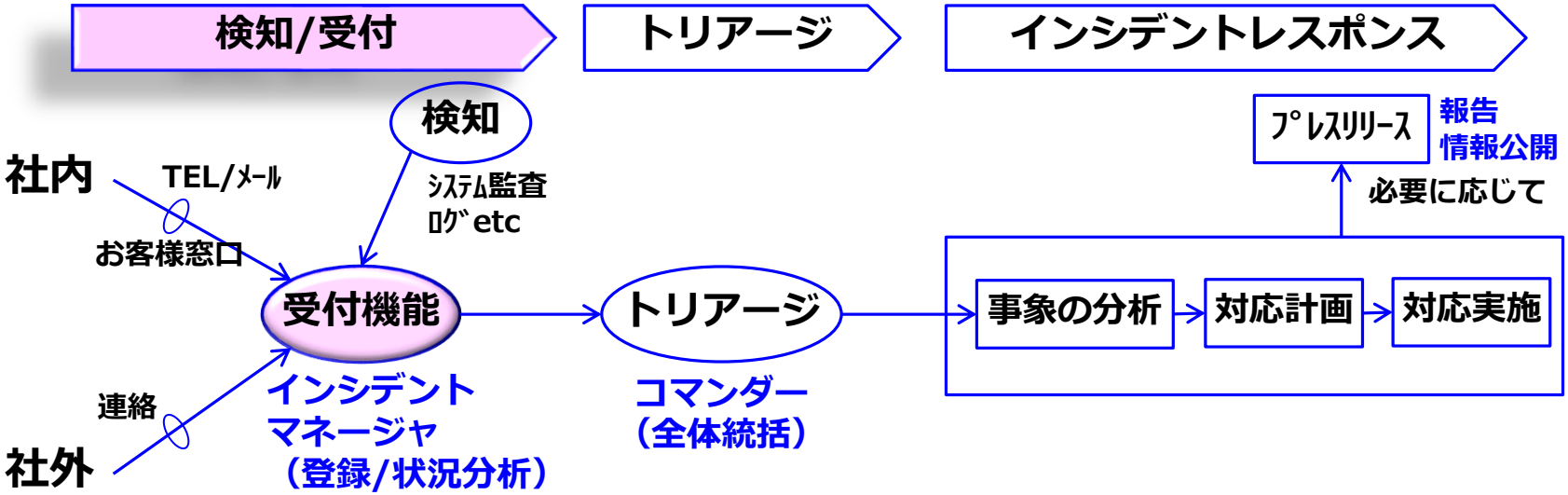
小さい組織は風通しが
よく意思決定が早い！！



基本的なCSIRT機能のスキルセット

担当	スキルセット	
	ヒューマンスキル	テクニカルスキル
受付 （外部/内部）	コミュニケーション能力 ・ヒアリング能力（傾聴） ・判断力（少ない情報から危険を察知）	サイバー対応の基礎スキル ・サイバー攻撃の仕組みの基本を理解 ・脆弱性情報とそれに対する対応する知識とプロセスを理解
CSIRT担当 （トリアージ）	コミュニケーション能力 ・調整能力（関連部署との調整＆指示） リーダーシップ ・判断力（リスク回避の為の即断） ・調整能力	サイバー対応の標準スキル ・サイバー攻撃の仕組みを理解 ・脆弱性情報に対応する知識とプロセスを理解し、攻撃を受けたダメージを最小限にするための指示
CISO （CSIRT責任者）	コミュニケーション能力 ・ネゴシエーション能力（経営者） リーダーシップ ・判断力（ビジネスリスクを最小限にするために判断）	サイバー対応の基礎スキル ・サイバー攻撃の仕組みの基本を理解 ・サイバー攻撃のリスクとビジネスへの影響を正しく理解
情報システム担当	コミュニケーション能力 ・調整能力（関連部署との調整） 向上心 ・前向きのスキルを磨き続ける能力	サイバー対応の標準スキル＆応用スキル ・サイバー攻撃の仕組みを理解 ・脆弱性情報とそれに対する対応する知識とプロセスを理解し、セキュリティログの分析ができる

組織内の基本的なCSIRT機能（受付機能）

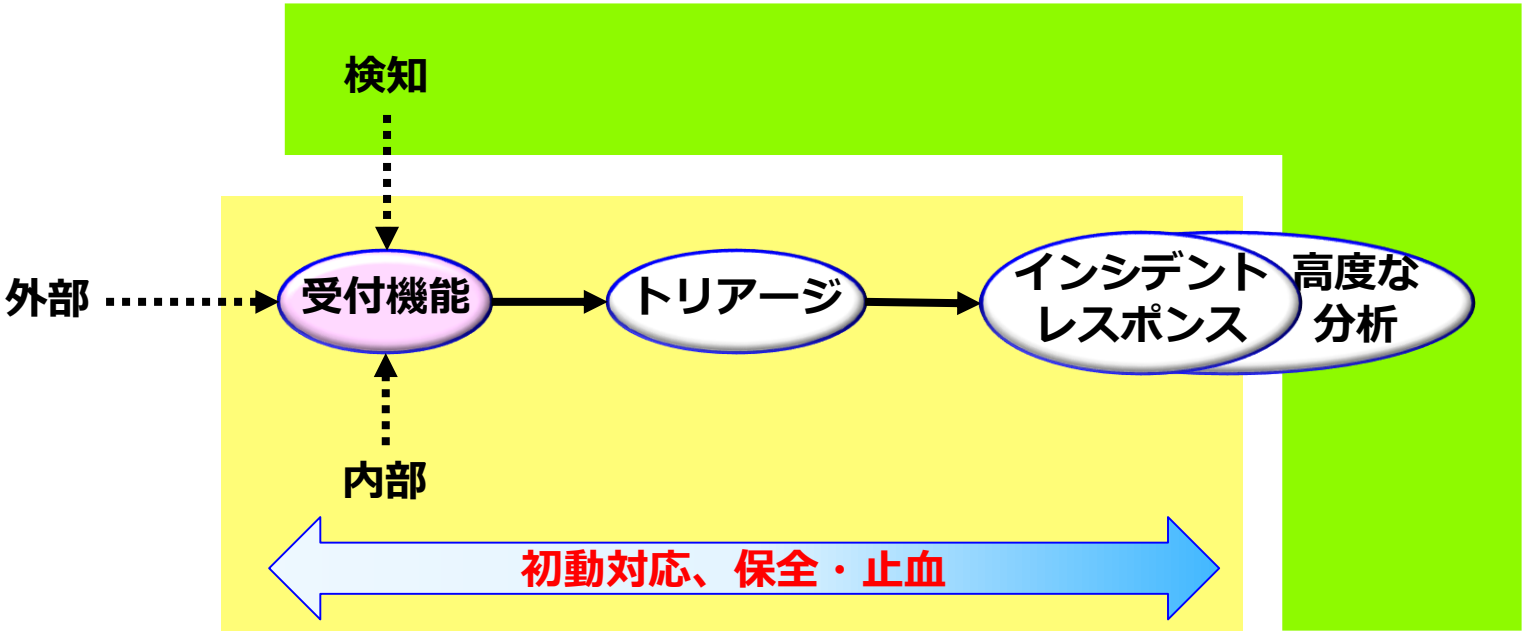


	受付機能	トリアージ機能	インシデントレスポンス対応
実装ｲﾒｰｼﾞ	既存のｲﾝｼﾃﾞﾝﾄ対応窓口にｻｲﾊﾞｰ対応機能をｱﾄﾞｵﾝする形で実装を行う ・独立組織で対応 ・組織横断で機能分担	一定のｻｲﾊﾞｰ系のｽｷﾙ保持者による判断が必要なため、既存の体制（ISMS事務局若しくは情報ｼｽﾃﾑ担当）にｱﾄﾞｵﾝする形で実装する	
必要機能	・社内/社外の情報窓口 ・ｲﾝｼﾃﾞﾝﾄﾁｹｯﾄ登録機能 ・ｲﾝｼﾃﾞﾝﾄ対応状況管理	・優先順位づけ、対応判断 ・情報共有、注意喚起 ・回答（対応の必要が無い場合）	・CSIRTで対応すべき事象の分析 ・対応計画 ・対応実施 ・ﾌﾟﾚｽﾘﾘｰｽ（必要に応じて）
備考	外部の対応窓口は一本化が必要。（連携出来ずに対応が遅れる可能性があるため）	ｺﾏﾝﾀﾞｰの位置づけとなるため、判断力＆決断力が求められる	

CSIRT機能（受付機能）の対応スクリプト（例）

ルート	連絡チャネル	通知情報	対応スクリプト
社内	**社員/P社員**	**誤って怪しい添付ファイルやリンク先をクリックした**	**・当該PCのNWからの遮断指示 ・インシデント受付＆コマンダーへディスパッチ**
	お客様窓口	間接的な異常情報の報告 （ネットに会社の機密情報or個人情報が漏れている）	・異常情報のヒアリング＆情報源の確認 ・インシデント受付＆コマンダーへディスパッチ
	検知	システム監査ログ等	・検知ログの内容を把握し、対応スクリプトを確認 ・インシデント受付＆コマンダーへディスパッチ
社外	公的機関	監視網にて攻撃を検知した	・攻撃情報のヒアリング＆確認 ・インシデント受付＆コマンダーへディスパッチ
	第三者	間接的な異常情報の報告 （ネットに会社の機密情報or個人情報が漏れている）	・異常情報のヒアリング＆情報源の確認 ・インシデント受付＆コマンダーへディスパッチ
検知	情シス	システムの負荷増大、DOS攻撃等	・情シスへのヒアリング ・インシデント受付＆コマンダーへディスパッチ
	外部サービス	SIEMサーバーやネットワーク機器、セキュリティ関連機器、各種アプリケーションから集められた**ログ**情報に基づいて、異常があった場合に管理者に通知する仕組み。「Security Information and Event Management」	・外部サービスからの情報把握 ・インシデント受付＆コマンダーへディスパッチ

自己完結すべき領域と外出し可能な領域



：自己完結すべき項目

：機能の外出しが可能

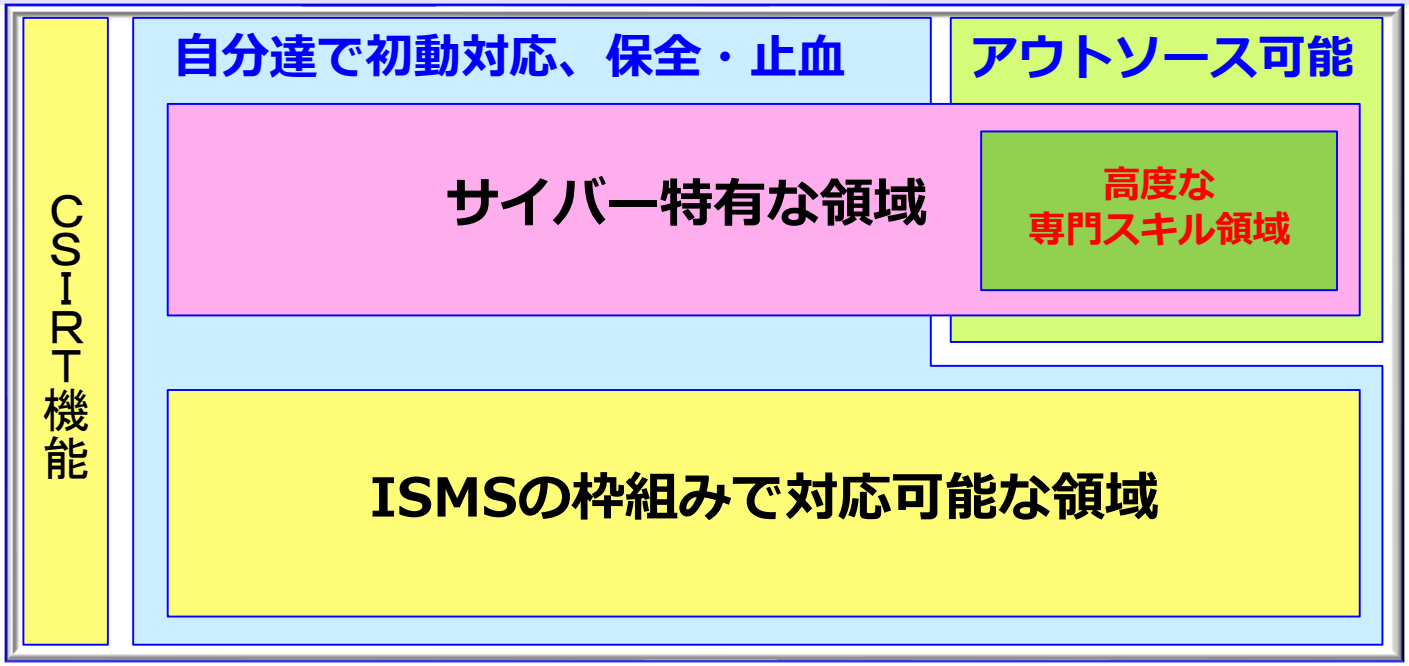
サイバーセキュリティに関する整理事項

（ISMSとCSIRTとの関係性）

協調

ISMS  CSIRT

ISMSの実装＋α（サイバー特有の視点を加味）



可視化

ISMSの実装で対応可能な領域とサイバー特有の領域

具体的な実装の例示（次頁～）

CSIRT機能	機能項目	対応管理策（1）	対応管理策（2）
インシデント事後対応の機能	・インシデントハンドリング ・コーディネーション ・コンピュータ・フォレンジックス　等	ISMSの枠組みで対応可能	サイバー特有の対応が必要 高度な専門スキルが必要
インシデント事前対応の機能（事前準備）	・セキュリティ関連情報提供 ・インシデント/セキュリティイベント検知 ・技術動向調査　等		
セキュリティ品質向上の機能（平時のとき）	・リスク評価分析 ・事業継続性、災害復旧計画作成・改変 ・セキュリティコンサルティング　等		

参考：ISMSの実装に加味するサイバー特有機能

機能	機能項目	ISMSの枠組みで対応可能	サイバー特有な対応（＋α）
インシデント事後対応	インシデントハンドリング	発生したインシデントへの 対応を行い、被害局限化・復旧のための活動 ・インシデントハンドリングの手順策定＆実施 ・トリアージ基準（合否判定、対応優先度） ・解決時に実施した手順等のエビデンス保存 ・情報共有や管理ツールの環境維持 ・再発防止手順	概ねISMSの枠組みで対応可能だが、下記の項目はサイバー特有の観点での補足が必要 **・インシデントハンドリングの手順策定＆実施** **・トリアージ基準（合否判定、対応優先度）**
	コーディネーション	組織を跨ったインシデント対応はISMSの枠組みでも発生するが、それぞれの責任でインシデントハンドリングを行うのはサイバー特有。	複数の組織（社内外）にて、それぞれの責任の下でインシデ ントハンドリングを行うことが必要となってくる場合があり、一貫した効果的なインシデントハンドリングを行うためには、CSIRT がインシデン ト全体を把握したコーディネータの役割を果たす必要がある。
	コンピュータ・フォレンジックス		インシデントが発生したコンピュータから、証拠となりうるデータを保存し、インシデントハンドリングを行う。高い専門性が要求され、専用ツールの準備が必要。 ①どのような被害を受けたか ②どこから侵入を受けたか ③誰が侵入者か
	オンサイトインシデントレスポンス		インシデントが発生したシステムやネットワークに対して、CSIRTが直接復旧作業を行う。（システムの運用担当者との責任分解点設定）
	インシデントレスポンスサポート	CSIRT がメール・電話・ドキュメントの提供等を行うことによるインシデントハンドリングを行う。	
	アーティファクトハンドリング		インシデントハンドリング時に発見された不審なプログラムを解析するサービス。不審なプログラムのソースコードの解析や、隔離した環境でのプログラムの挙動解析を実施し、不審なプログラムがインシデントの原因であるかどうかの調査を行う。専門のスキルを持ったメンバのCSIRTへの配置や、他のNWから隔離されたアーティファクトハンドリング専用の設備が必要。

ISMSの実装にサイバー特有機能加味する事例

注：各組織の状況によりISMSの実装レベルが異なることから標準的な参考例として提示

参考：ISMSの実装に加味するサイバー特有機能

機能	機能項目	ISMSの枠組みで対応可能	サイバー特有な対応（＋α）
インシデント事前対応の機能(事前準備)	セキュリティ関連情報提供	セキュリティ情報をサービス対象に情報提供するサービスである。提供する情報を以下に例示する。 - CSIRT の活動内容周知/連絡先周知 - ポリシー/プロシージャ/セキュリティ関連のチェックリスト - 流行しているウイルス/ワーム情報や攻撃手法 - インシデントレスポンスの一般的手法 - インシデント統計情報	通常の事務局対応作業のプロシージャにサイバー対応の情報を盛り込んで発信を行う
	脆弱性情報ハンドリング	ISMSの枠組みで実施することも可。	SW/HWの利用状況を把握し、関連する脆弱性情報を分析し、入手サービス対象へ伝達する ・情報先の管理と適切な情報提供 ・対処要否の判断、対応手順の策定、実施
	インシデント/セキュリティイベント検知		インシデント/セキュリティイベントなどを検知するサービス。 検知方法は、IDS やハニーポット の設置、各種サーバ群のログの解析、P2P ファイル共有アプリケーションを経由した情報漏えい検知のための専用環境等がある。
	技術動向調査	セキュリティ[illegible]のための技術やインシデント検知技術、もしくは侵 入技術等の最新のセキュリティ技術動向調査や目利きを実施し、サービス対象への有用性を確認するサービス。	通常事務局対応作業の延長でサイバー特有の技術動向を盛り込む。
	セキュリティ監査/査定		ドキュメントの確認やペネトレーションテストを通じて、監査/査定 するサービスである。
	セキュリティツールの開発		CSIRTやサービス対象が利用するセキュリティツールを開発するサービス。 例：新しいインシデント検知ツールや、暗号化技術を容易に利用することのできるスクリプトや、自動化さ れたパッチ配信の開発など

ISMSの実装にサイバー特有機能加味する事例

注：各組織の状況によりISMSの実装レベルが異なることから標準的な参考例として提示

参考：ISMSの実装に加味するサイバー特有機能

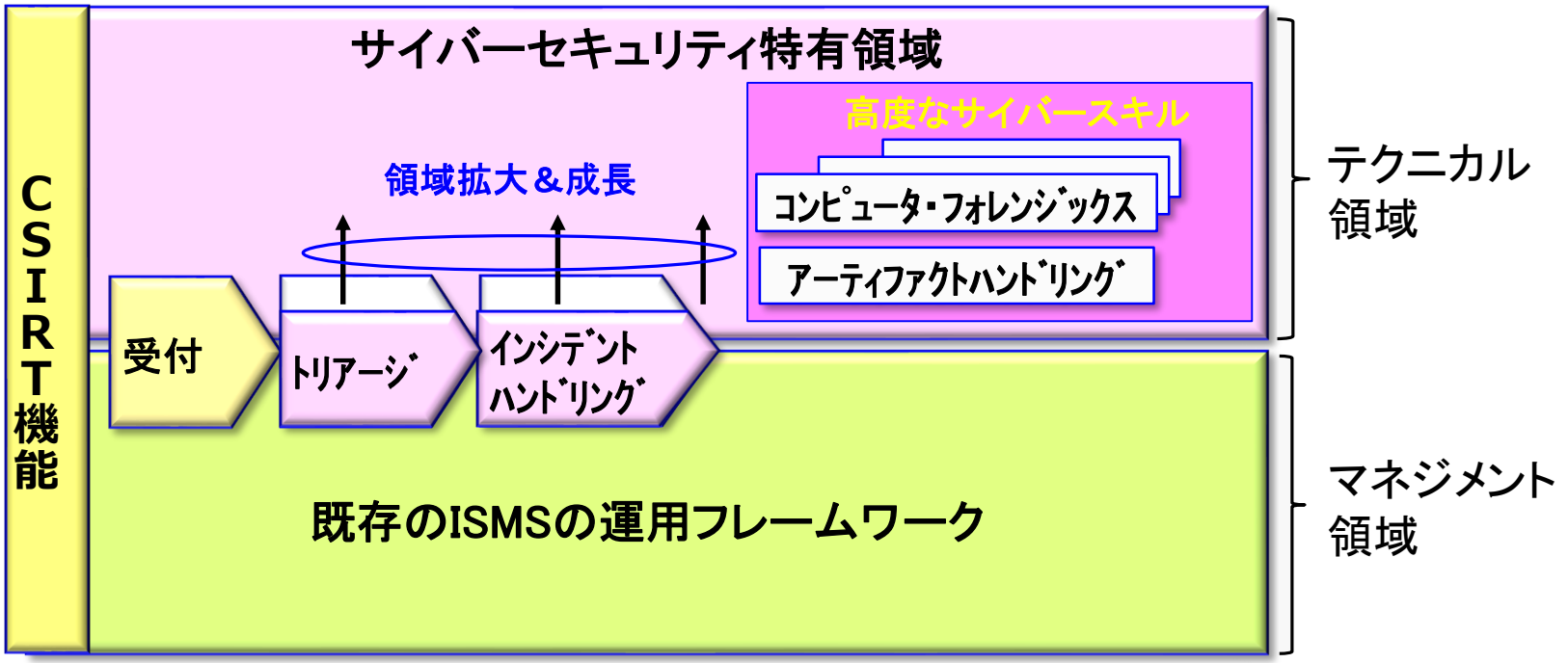
機能	機能項目	ISMSの枠組みで対応可能	サイバー特有な対応（＋α）
セキュリティ品質向上の機能（平時）	リスク評価分析	企業や対象となる情報システムの機密性、完全性、可用性を阻害 する様々なリスクを洗い出し、その影響度を分析するサービス。（現状のリスクの認識と、リスクを受容範囲にメネジメントする） ・情報資産の洗いだし、リスク分析手順の策定 ・リスク分析結果に基づく是正対応	サイバー特有な項目の盛り込み
	事業継続性、災害復旧計画作成・改変	通常のBCPに加えてCSIRTとしてのインシデントレスポンス機能を事業継続性、災害復旧計画として反映させるサービス。	サイバー特有の特徴として、外部への情報漏洩の疑いがある場合は自らNWの遮断等を実施することで、被害拡大を防ぐ判断が必要となること。 ・BCPにサイバー対応計画を反映 ・フィージビリティの確認の演習の実施
	セキュリティコンサルティング	ISMSの実装にサイバー特有機能加味する事例	CSIRT としてのノウハウをサービス対象の事業へ反映させるための コンサルティングを行うサービス。 ・情報システムの企画設計、運用中のシステムに対するセキュリティ相談窓口の設置＆実施 ・知見の体系化＆蓄積（文書化含む）
	セキュリティ教育/トレーニング/啓発活動	CSIRTでのノウハウや、そのノウハウを反映させたポリシー・プロシージャ等をサービ ス対象に教育やトレーニング、啓発活動を行うサービス。 ・社員/P社員にセキュリティ啓発/教育計画を策定し、実施	・通常の事務局の営みで実施するセキュリティ研修に加えて、サイバー対応の項目の盛込み
	製品評価・認定		製品・ツール・プロダクト・サービス等に関して、それらをサービス対 象がセキュアに利用できるものかどうかをCSIRT が評価・認定するサ ービス。

注：各組織の状況によりISMSの実装レベルが異なることから標準的な参考例として提示

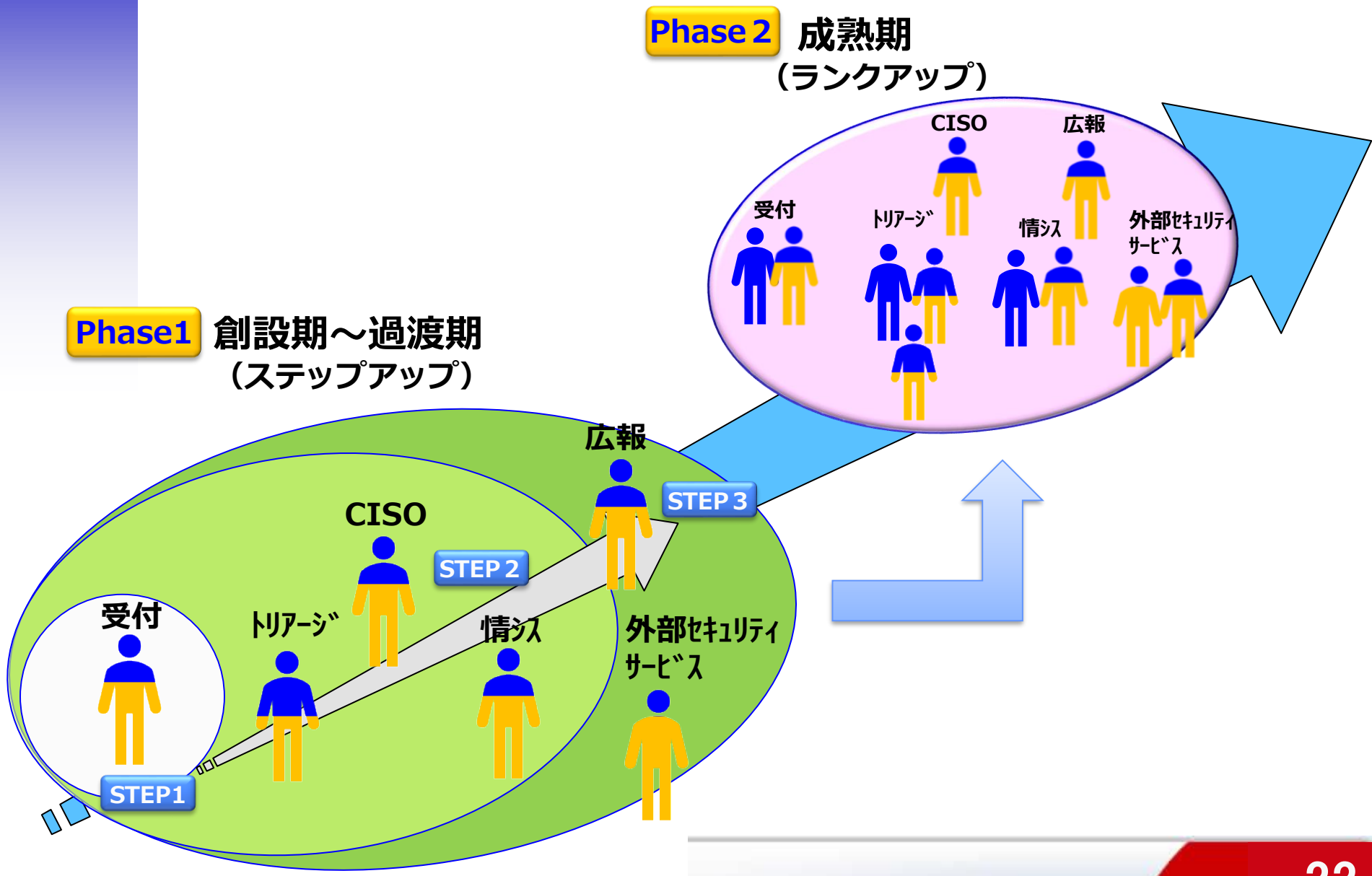
CSIRT機能導入におけるSTEP論（スモールスタート）

STEP1：まずは入り口となる受付機能から始める
STEP2：基本的な機能の実装(ﾄﾘｱｰｼﾞ、ｲﾝｼﾃﾞﾝﾄﾊﾝﾄﾞﾘﾝｸﾞ等)
STEP3：サイバー対応スキルUPを図りながら、組織に必要な対応領域を拡大

・無理をせず、身の丈にあった実装を！
・ISMS構築＆運用＋α（サイバー特有のもの）を追加実装
・フォレンジックス等の高度なサーバースキルはアウトソーシングを視野に！



CSIRT機能導入におけるSTEP論



事例研究（Part2）

クラウド利用時のリスク対応

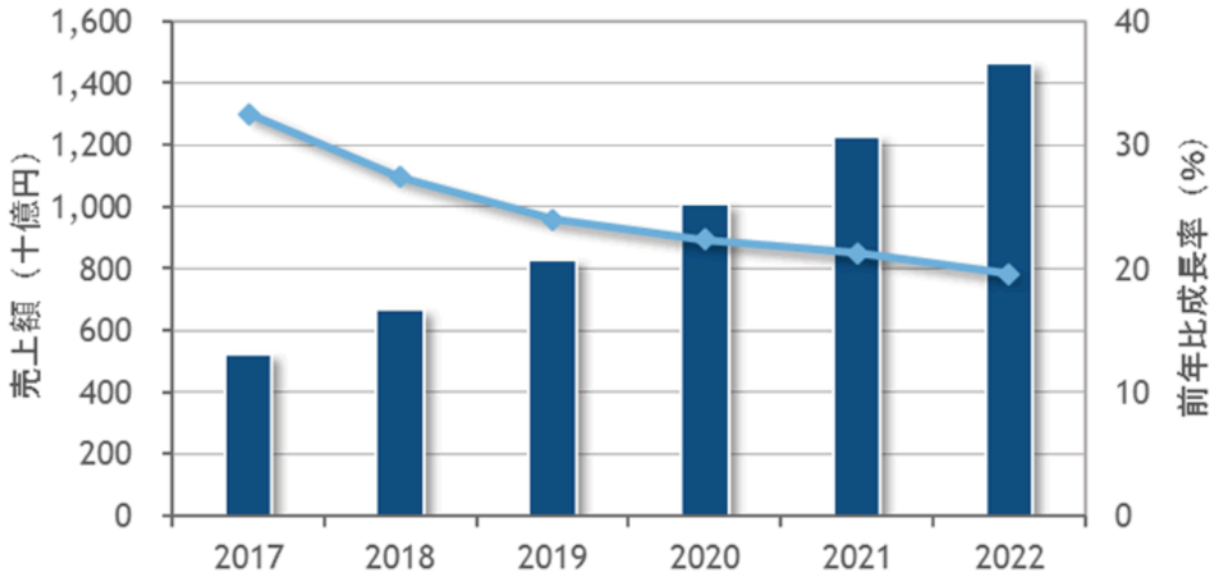
参考： パブリッククラウドサービス市場の拡大

国内パブリッククラウドサービス市場予測を発表

2018年10月1日
IDC Japan株式会社

- **2018年の国内パブリッククラウドサービス市場は、前年比27.4%増の6,663億円となる見込み**
- **2022年の市場規模は、2017年比2.8倍の1兆4,655億円になると予測**
- **「従来型ITからクラウドへの移行」と「DXアプリケーション」が、国内パブリッククラウドサービス市場の成長を促進し、同市場は高い成長を継続**

<参考資料>
国内パブリッククラウドサービス市場 売上額予測、2017年～2022年



https://www.idcjapan.co.jp/Press/Current/20181001Apr.html

ISMS事務局の悩み・・・（クラウド利用）

ビジネス優先、効率優先でクラウド導入が加速・・・

クラウド抜きでは
ビジネスにならない、
大丈夫か？？？
リスク対応はどうする・・・

利用部門が勝手に導入
＆　全体の導入状況が見えない！・・・

情シスのコントロールが
効かない＆把握出来ない・・・

リスクアセスメント
は大丈夫？

クラウド特有のスキル、
ノウハウが不足・・・

社内ルールとの乖離
（お客様指定等でファイル共有
などを利用・・・）

機密情報（個人情報含む）が日本リージョン以外に・・・

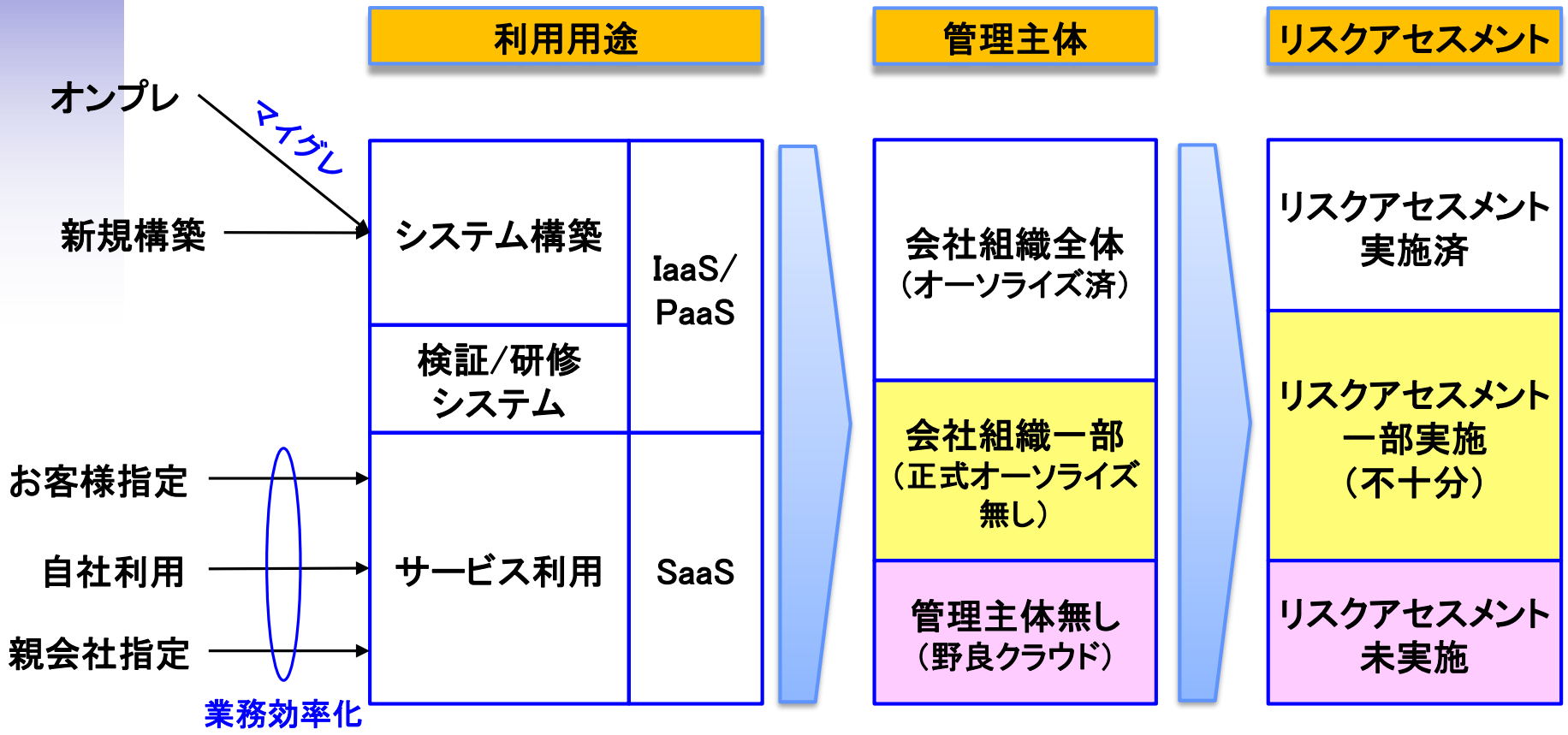
組織としてどうバランスを保つか？

課題設定とGoalイメージ（クラウド利用）

課題設定	テーマ終了時のGoalイメージ
・クラウド/サービスファーストでリスク無視 ・利便性重視傾向（リスク受容ではなく無視） ・有効なリスクアセスメントが出来ていない ・クラウド利用のリスクの可視化	クラウド利用時のリスクの可視化 & リスクの可視化＆対応プロセスの提案
・クラウド利用＆サービス利用が第一優先（ビジネスメリットとリスクのバランス判断がない） ・企画からサービス開始までの時間が短い ・利用部門で自由に導入ができ、リスクが見え難い、管理し難い ・野良クラウドを把握するのが難しい	・クラウド利用時のリスクの可視化 ・クラウド利用のためのガイドライン（簡易版）によるベースラインの設定 ・社内でのクラウド利用の手続き＆モニタリングプロセスの策定 ・運用上の注意事項の明示＆研修

クラウド利用の全体像 （可視化のアプローチ）

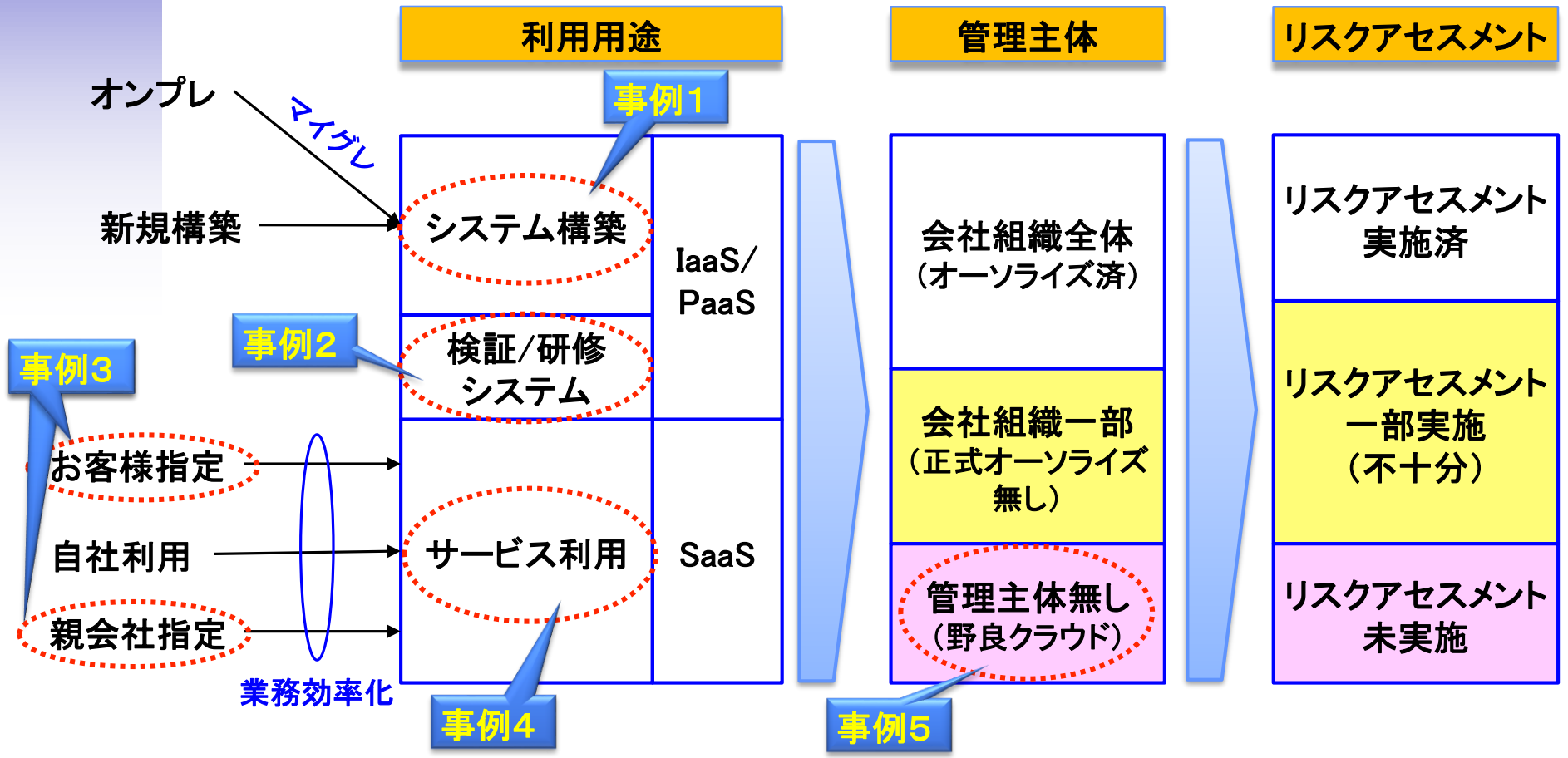
利用用途、管理主体、リスクアセスメントの有無の観点で整理



※：黄色＆ピンクの網掛けは危険ゾーン

クラウド利用の全体像　（リスク事例）

リスク事例について次ページ以降のスライドにて解説する

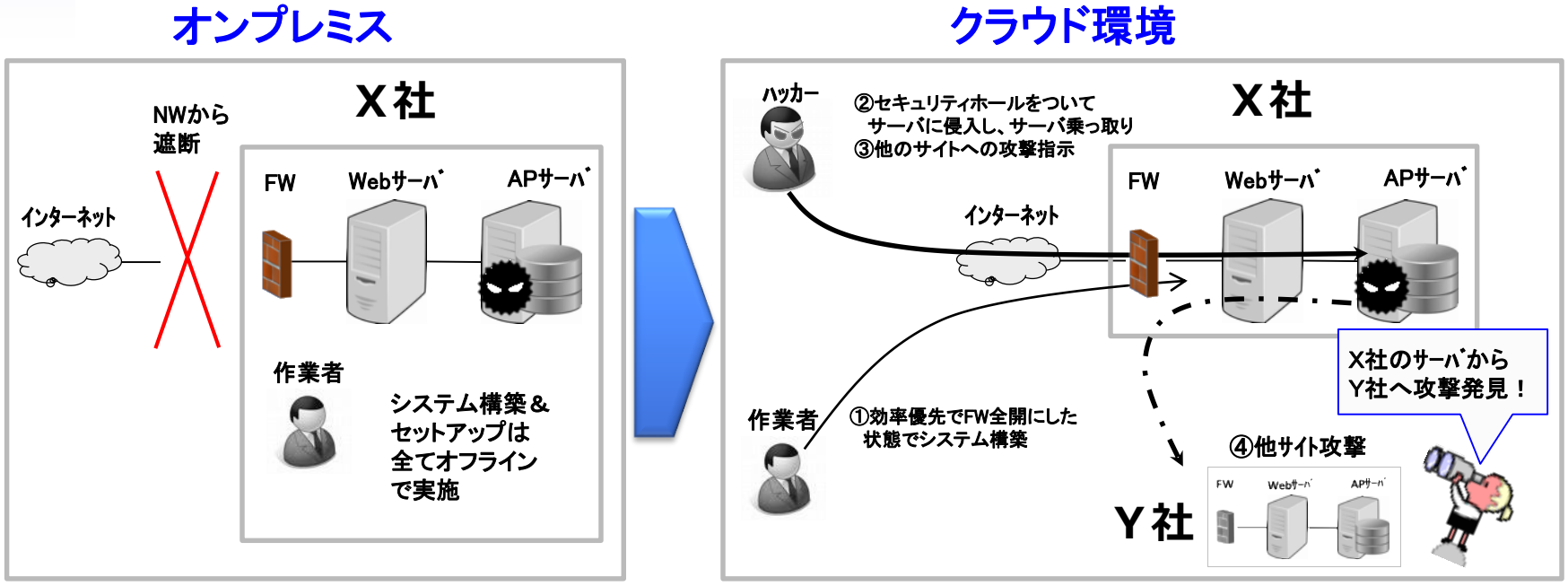


クラウド利用の全体像　（リスク事例１）

○クラウド環境上でのシステム構築時のリスク（落とし穴）

①クラウド上では常にNWを介してのサーバ構築となる。その為、効率性を優先しFWのポリシー設定を全開にして作業が実施されることがある。
②ハッカーはわずか5分程度の全開にしている間にサーバに侵入し、乗っ取りが完了（ハッキングされる危険性はほぼ100%・・・）
③乗っ取ったサーバに対して攻撃指示。
④他のサイト（同一クラウドサイトの他のVMなど）への攻撃を実施

→ 他のサイトから見ると加害者となり、企業の信用失墜！

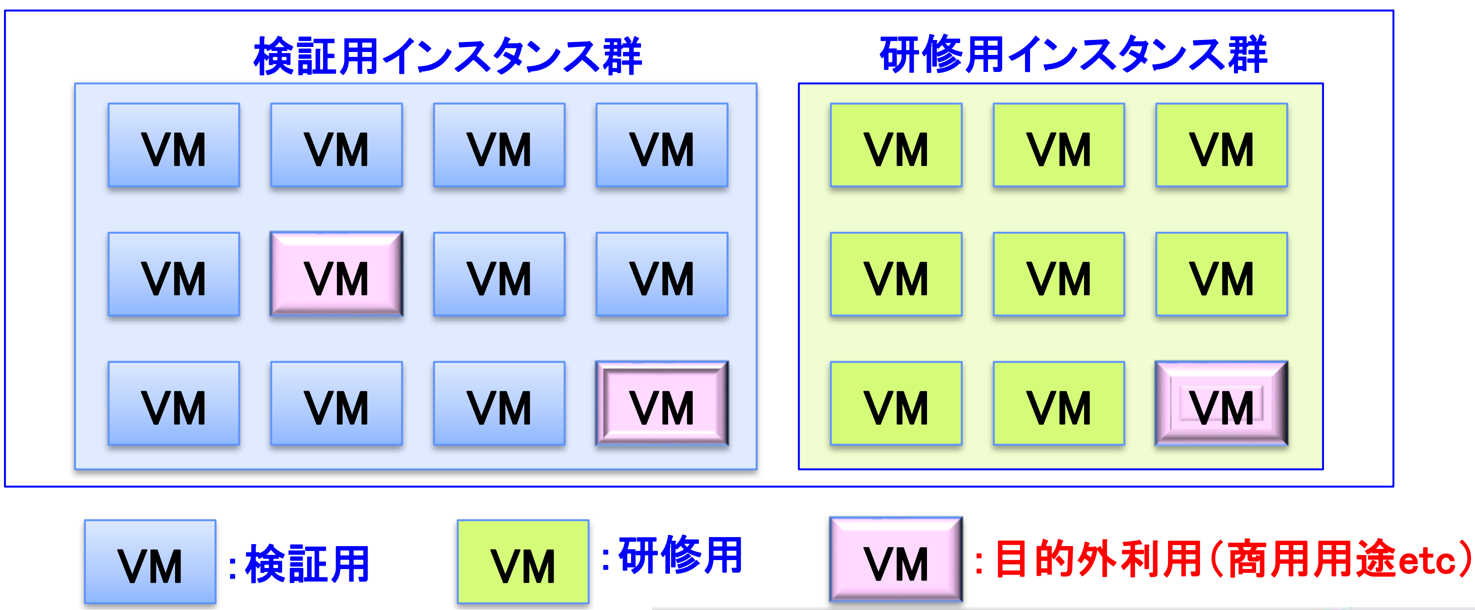


クラウド利用の全体像　（リスク事例２）

○検証/研修システム利用時のリスク（落とし穴）

- ・検証/研修用としてのクラウド利用では機密情報は取り扱わないという妄想・・・
- ・セキュリティ対策がおざなりになりがち
- ・作成→利用→削除というプロセスを繰り返すため、きちんとした管理プロセスが馴染まない
- ・全体を管理するプロセスが作り難い、管理者が不在のケースが多々・・・
- ・管理が自由なため、目的外利用などの不正利用が発見しにくい
  → 実際には会社情報を書き込んだり、商用目的との境が曖昧になりがち（手軽に利用可）

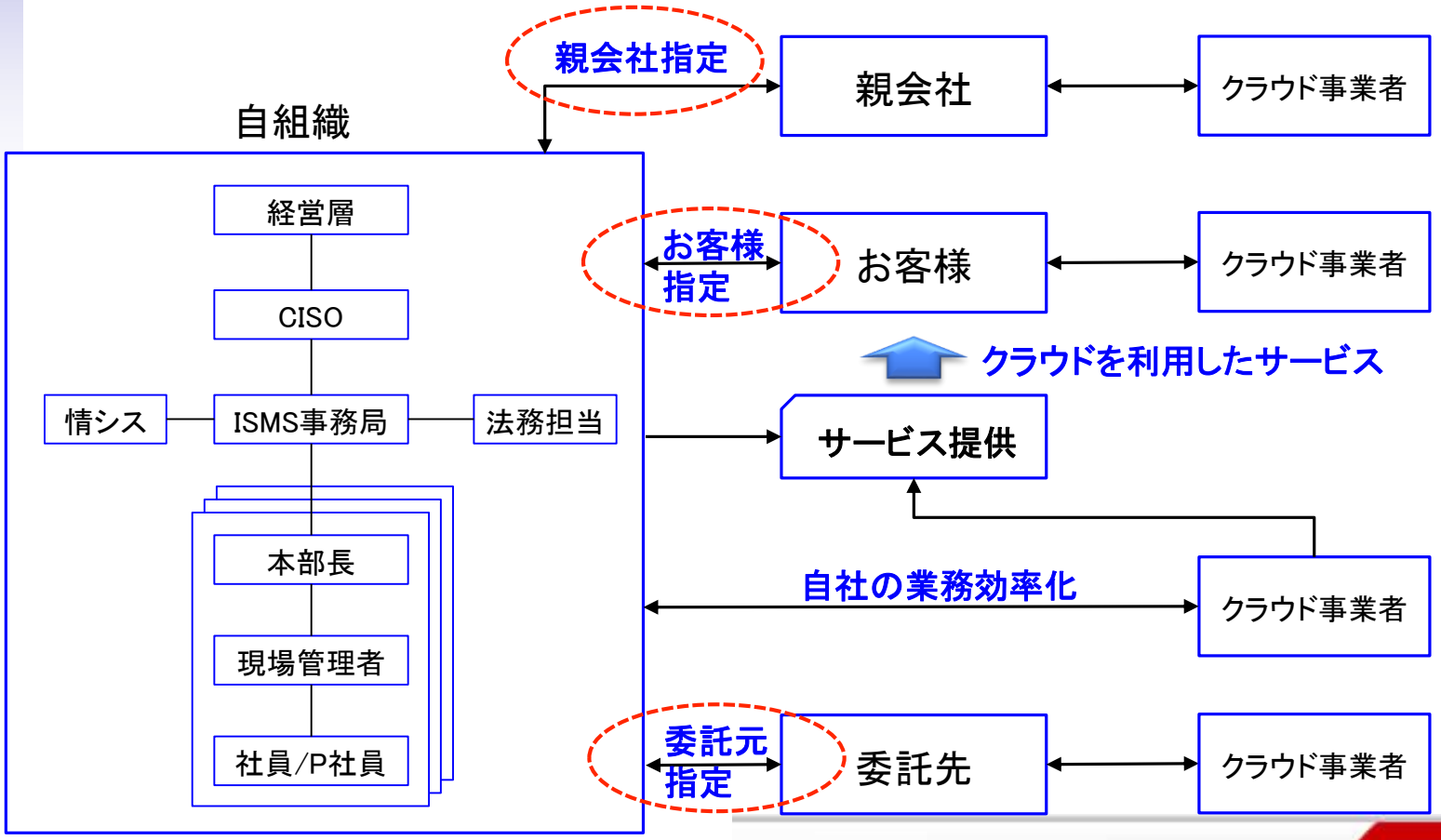
無いはずの機密情報が漏えいし、企業の信用失墜！



クラウド利用の全体像　（リスク事例３）

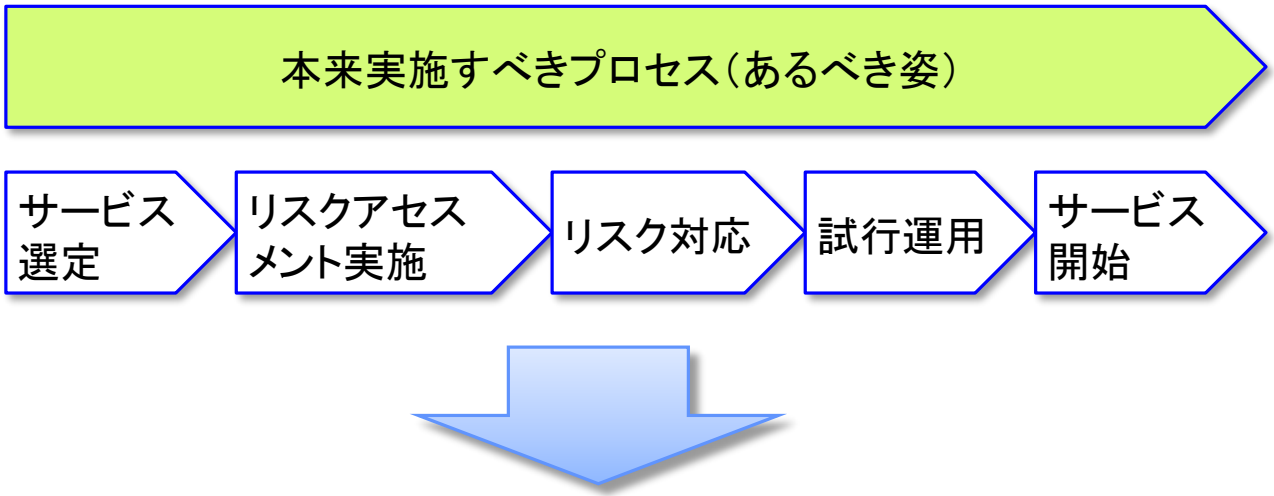
ステークホルダー関係図（お客様/親会社/委託元指定による利用）

・クラウド利用案件の増加（自社利用、お客様/親会社指定、サービス構築案件等）
・クラウド化に伴い客先常駐ではなくバーチャルな組織構成のプロジェクトが増加・・・



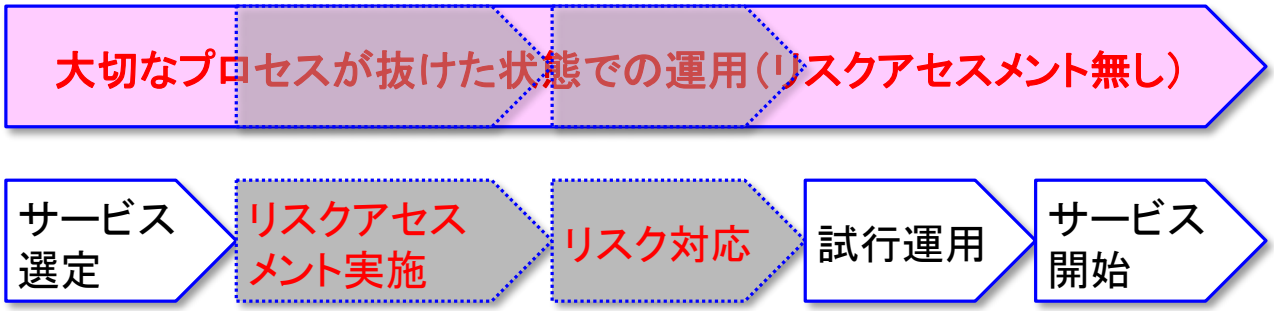
クラウド利用の全体像　（リスク事例３）

○サービス利用（お客様指定/親会社指定）時のリスク（落とし穴）



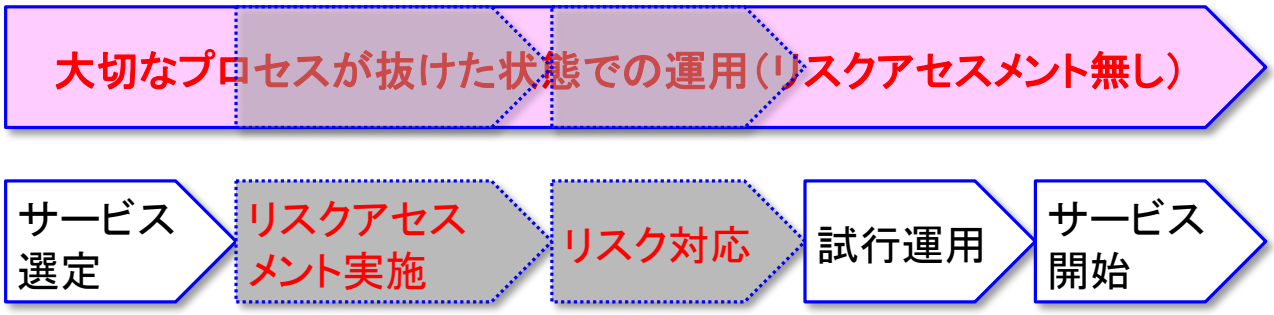
○お客様/親会社の指示なのでリスクアセスメント無しで利用

・利用規約、利用マニュアル無しで利用することで目的外利用が発生
・デバイスに紐づいていないので私有デバイスで利用可能



クラウド利用の全体像　（リスク事例３）

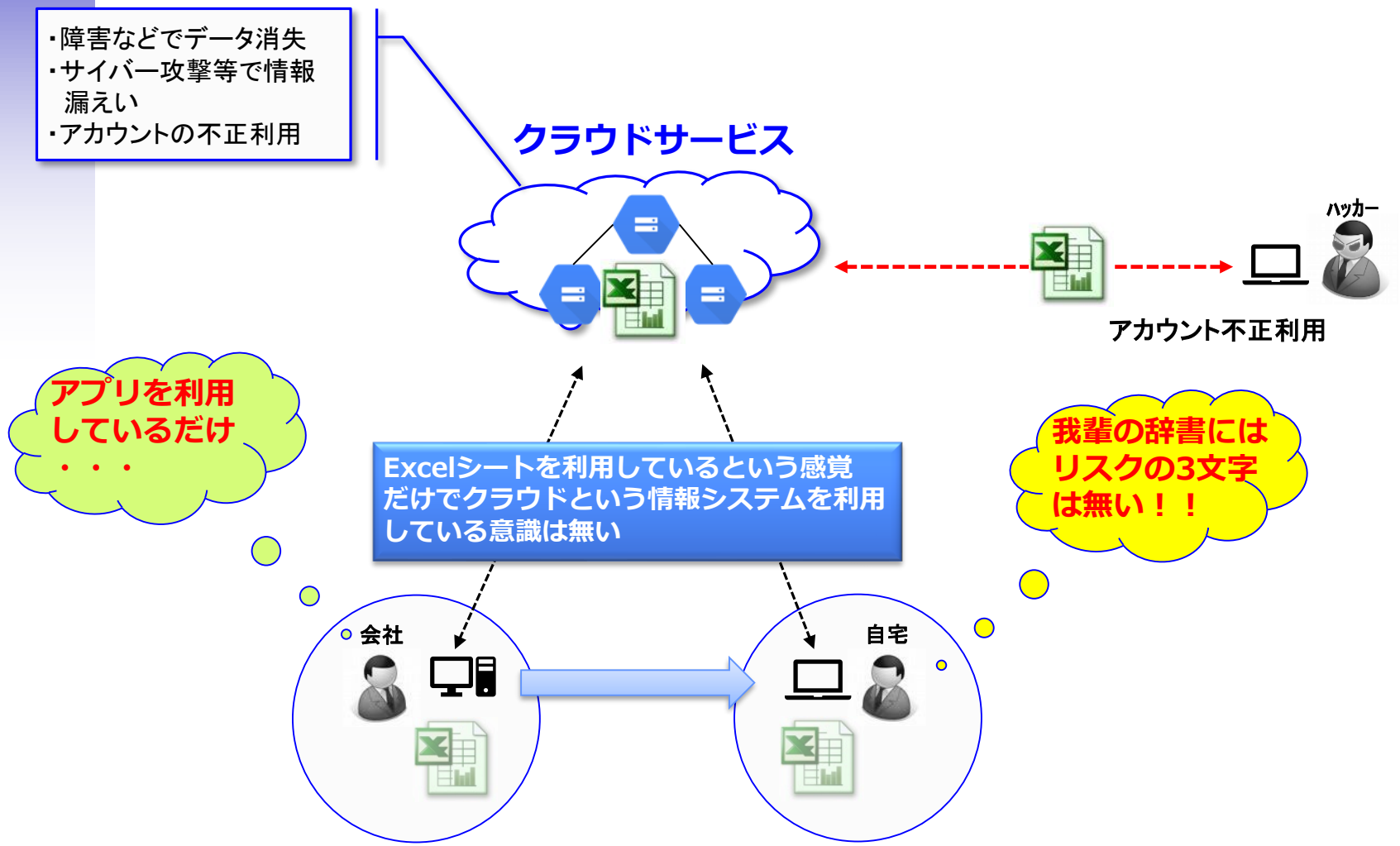
○お客様/親会社の指示なのでリスクアセスメント無しで利用



発生事象	事例紹介
利用規約、利用マニュアル無しで利用することで**目的外利用**が発生	当初の想定する利用範囲を超えて使用するリスク ・チャットツールや共有ファイルサービス等で禁止された**機密情報の利用** ・許可されているプロジェクト案件以外でも**無許可利用** （利用範囲の拡大）
デバイスに紐づいていないので**私有デバイスで利用**可能	クラウドサービスなのでアカウントに紐づいており、会社貸与のデバイス以外でも利用可能。 ・私用デバイスを介した**機密情報の漏洩リスク** ・アカウントの切り替えで会社契約のサービスと個人契約のサービスの切り替えが簡単に実施できるため、誤用の危険性

クラウド利用の全体像　（リスク事例４）

クラウド利用時における一般ユーザの認識レベル



クラウド利用の全体像　（リスク事例５）

○野良クラウドの定義とリスク（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。

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（案）

管理主体	情シス把握（正規手続き）	部門のみ把握（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	目的外のリスクアセスメントは未	リスクアセスメントが不十分		リスクアセスメントは未実施	リスクアセスメントは未実施
利用目的範囲内外（承認時）	利用目的内	利用目的外（検証環境を拡大利用）	利用目的内	利用目的外（検証環境を拡大利用）	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

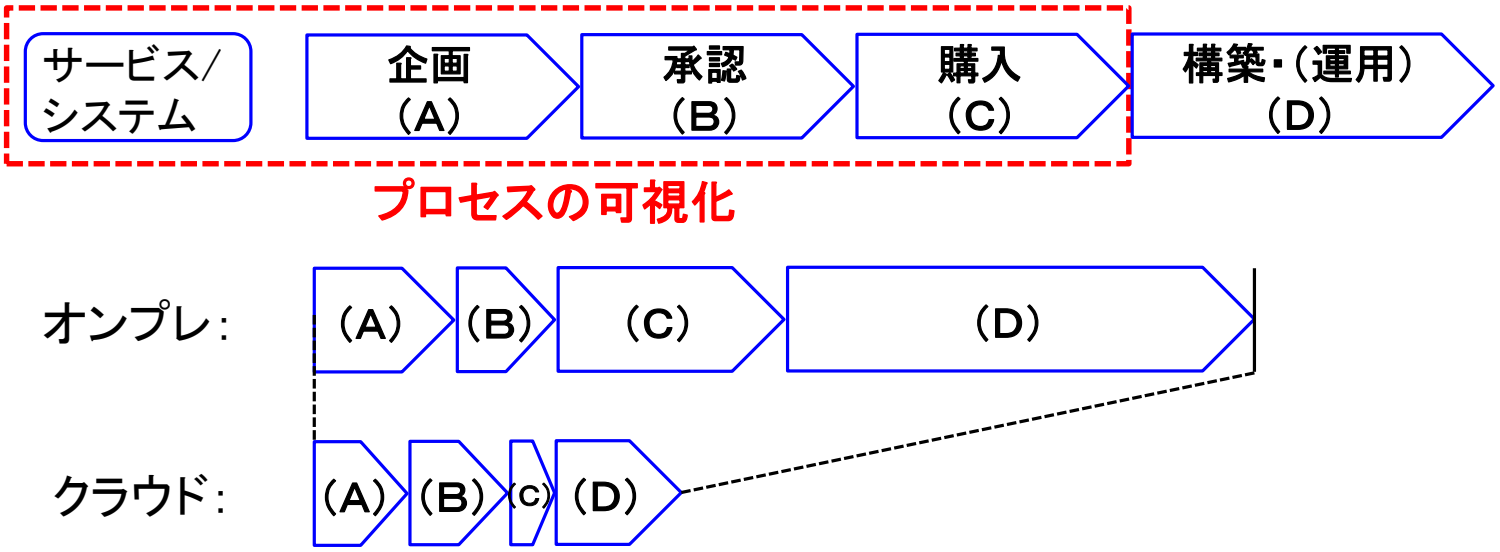
小 ← リスク → 大

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（申し込んだその日か使える）、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
クレジット払いの場合に実態との関連付けが見えにくい・・・）



※：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（クラウド化で不要となる作業項目）

オンプレ	企画（A）	承認（B）	購入（C）	構築・（運用）（D）
経営層		ビジネスの実現性＆セキュリティについて審議＆承認		
契約/経理			購入手続き＆支払い	
法務				
情シス	ラックの確保＆システム要件確認			工事調整
事業本部	事業部内承認	システムの開発付議		
部門（現場）	システムの企画/立案 DCのラックの確保		購入決裁処理 ＆回線手配	購入機器の搬入＆ラッキング システム構築

クラウドにより不要となる作業項目

クラウド	企画（A）	承認（B）	購入（C）	構築・（運用）（D）
経営層		ビジネスの実現性＆セキュリティについて審議＆承認		
契約/経理			購入手続き＆支払い	
法務				
情シス	~~ラックの確保＆システム要件確認~~			~~工事調整~~
事業本部	事業部内承認	システムの開発付議		
部門（現場）	システムの企画/立案 ~~DCのラックの確保~~		購入決裁処理 ~~＆回線手配~~	~~購入機器の搬入＆ラッキング~~ システム構築

野良クラウド発生メカニズム（正規の手続きの抜け穴）

正規の手続きをしなくても利用することが可能・・・

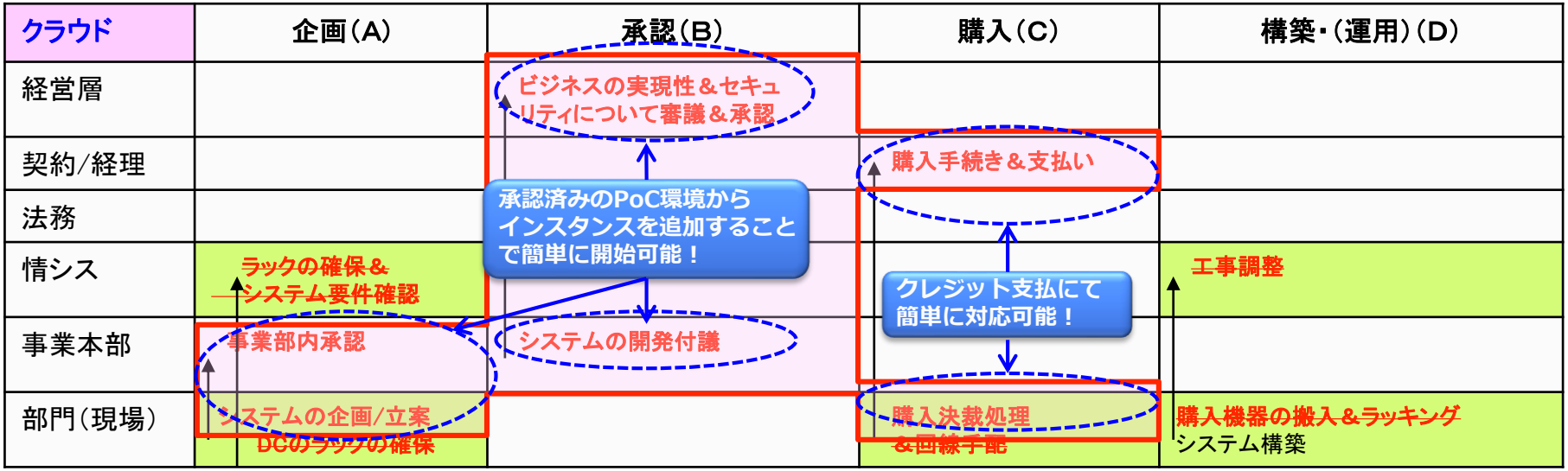
○利用開始の承認手続きをしなくても気がつかない

- 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

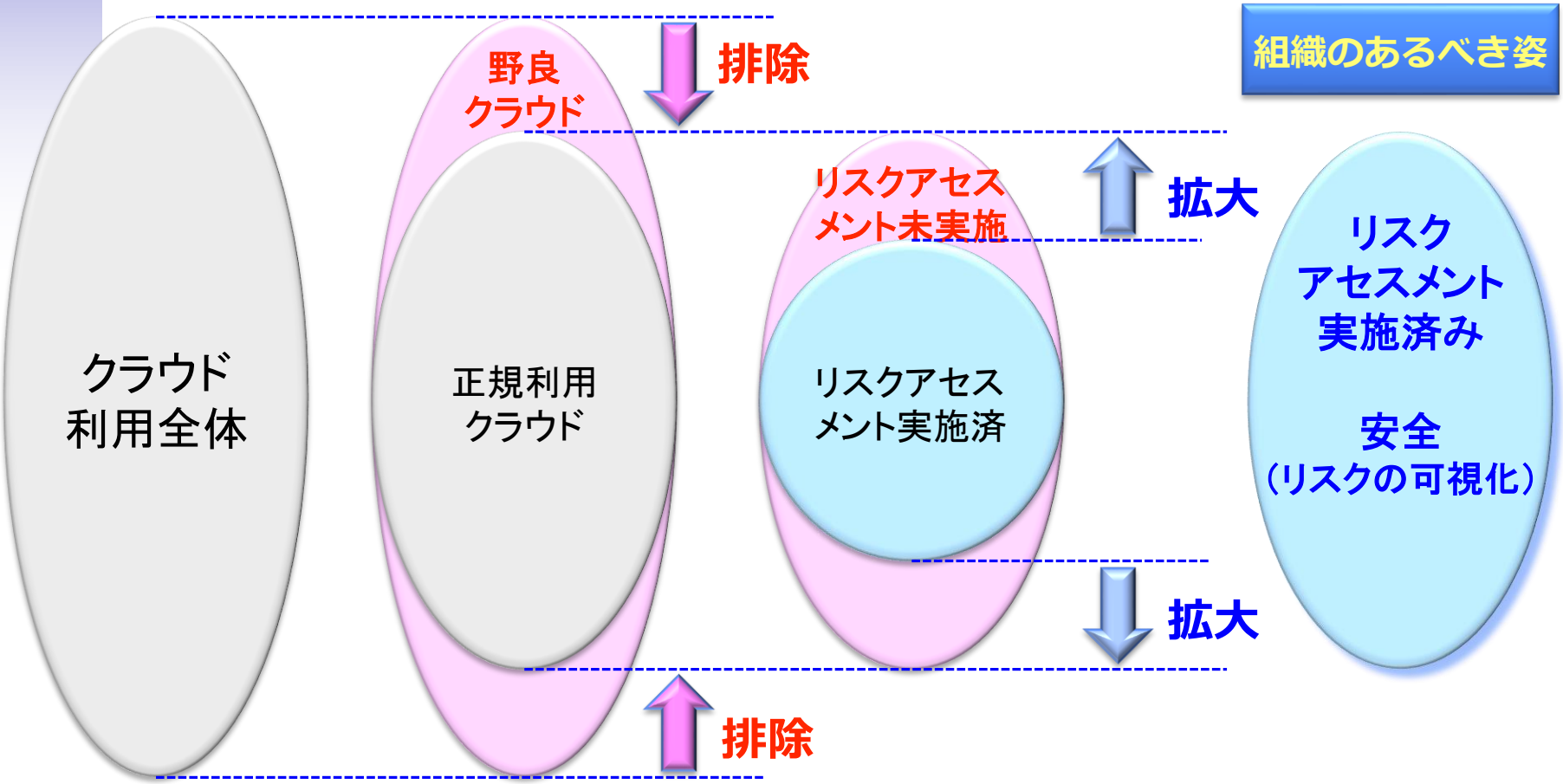
- 利用開始前に把握することも運用フェーズでも難しい

○リスクアセスメントを実施していないので大きな潜在リスクが多数



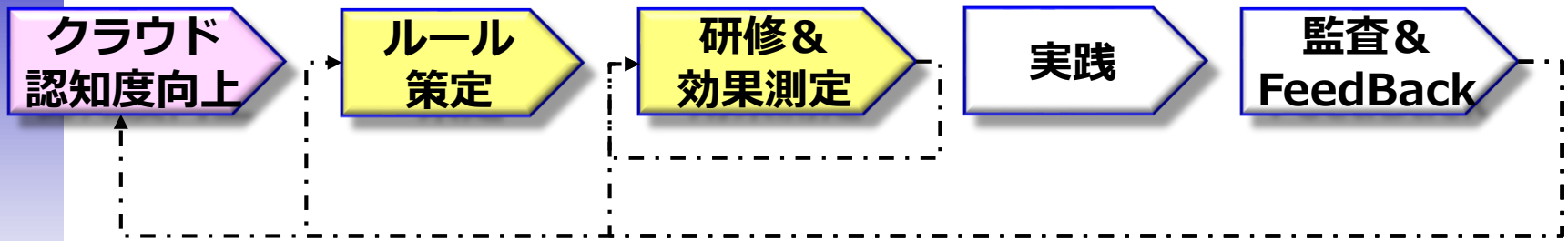
クラウド利用時のリスクアセスメント

野良クラウドの排除　＆　リスクアセスメントの拡大



クラウド事例のまとめ

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
- ルールブックの策定（申請/承認）
- 罰則規定

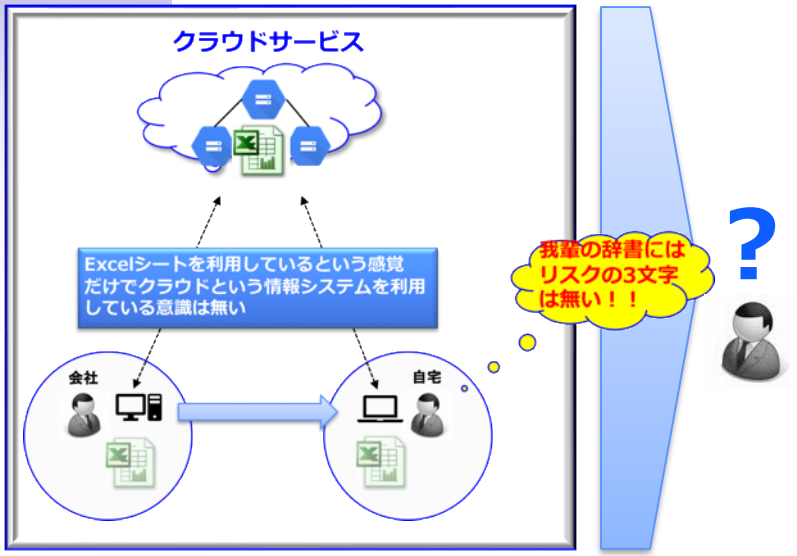
- 社内ルールの理解
- インシデント発生時のビジネスインパクトの理解
- リスクアセスメントの実践研修
- ルール逸脱時の罰則理解
- 効果測定結果に基づく再研修

- 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

- 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）→野良ｸﾗｳﾄﾞの検出含む
- 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

- 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

遵守

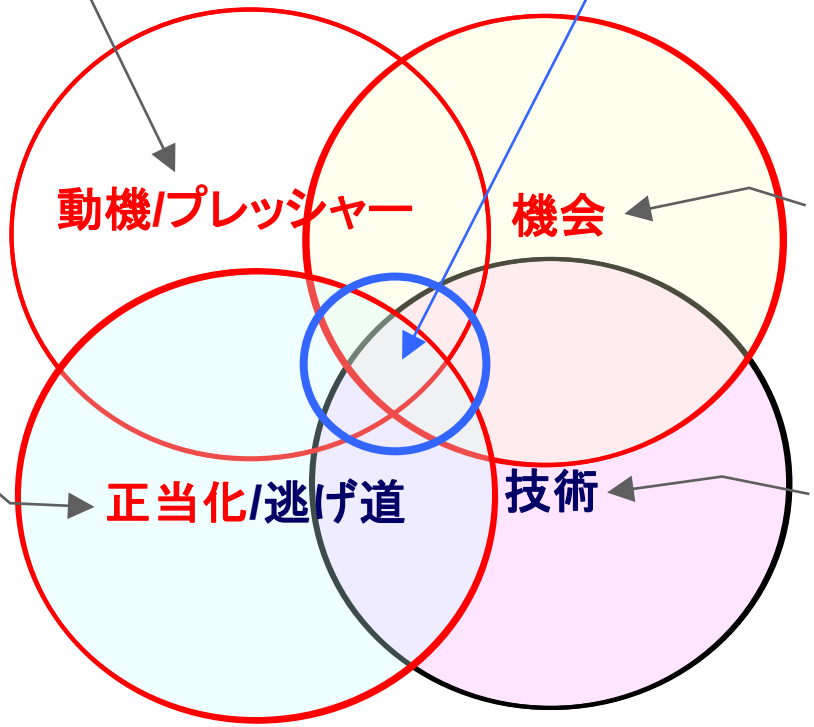
- 申請～承認
- 許可範囲での利用
- リスクアセスメントの実施
- クラウド利用の登録＆管理

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

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）

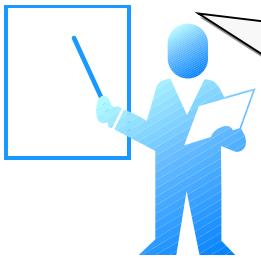


四要素が重なっている部分で問題が発生し易い。

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）

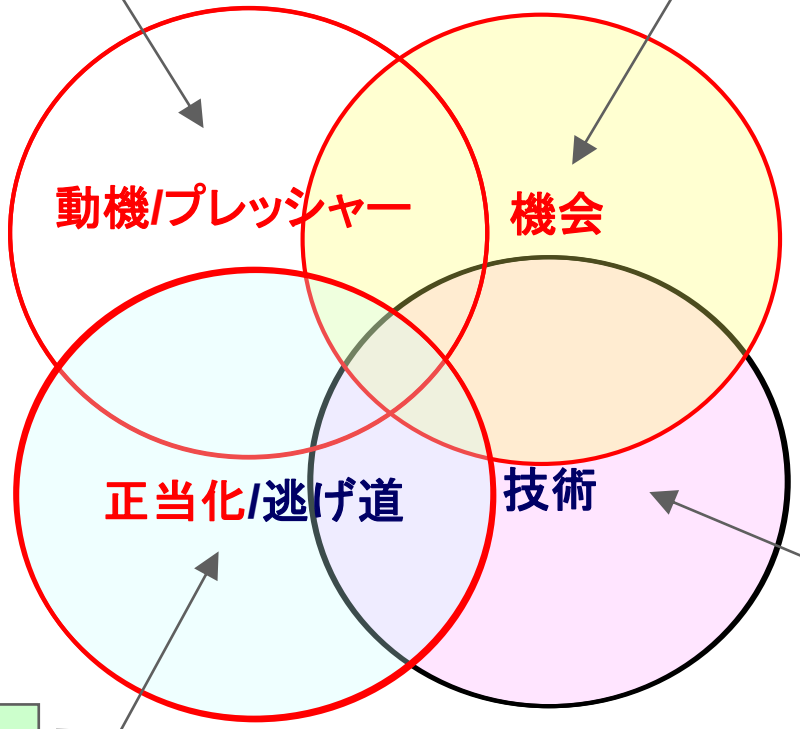


不正のトライアングル（赤〇の項目）は、米国の犯罪学者であるD.R.クレッシーが、人間（犯罪者）の心理面を研究して導き出した理論ですが、情報セキュリティの面からみると、トライアングル理論に、「技術」や「逃げ道」などを追加することで、より効果的にインシデントを防止できる可能性があります。

ルールから逸脱しやすい要因とは？

・面倒な手間を掛けずに利用可能
・すぐに成果/効率化を求められる

・承認機能が働きにくい（設備投資が発生しない）
・チェック機能が働かない（見つからない）
・クレジット払いで簡単（無料枠もあり）
・Anywhere、Anytime利用可能



◎ ルール可視化
& チェック

・お客様指定
・クラウドファーストだから
・規定/ルールに禁止事項がない
・他の社員もやっている

・技術があればルールの抜け穴で不正利用

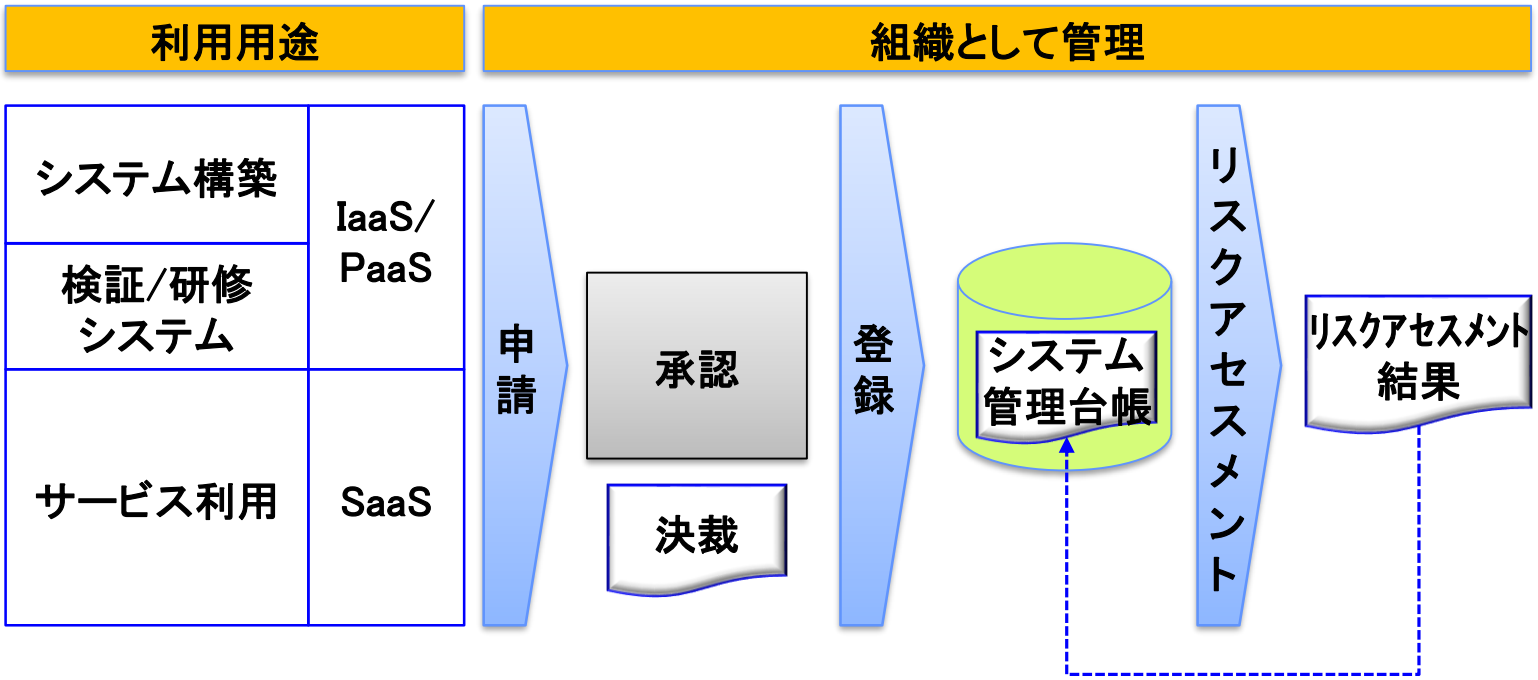
解決策として高度な技術で防御
CASB（＊1）が注目

CSCとCSPの間にCASBを配置し、単一のコントロールポイントを設けて、認証／シングルサインオン、アクセス制御、データ暗号化、ログ取得、マルウェア対策といった、クラウド・リソースへのアクセスに関するセキュリティ・ポリシーを適用

＊1：Cloud Access Security Broker 通称：キャスビー

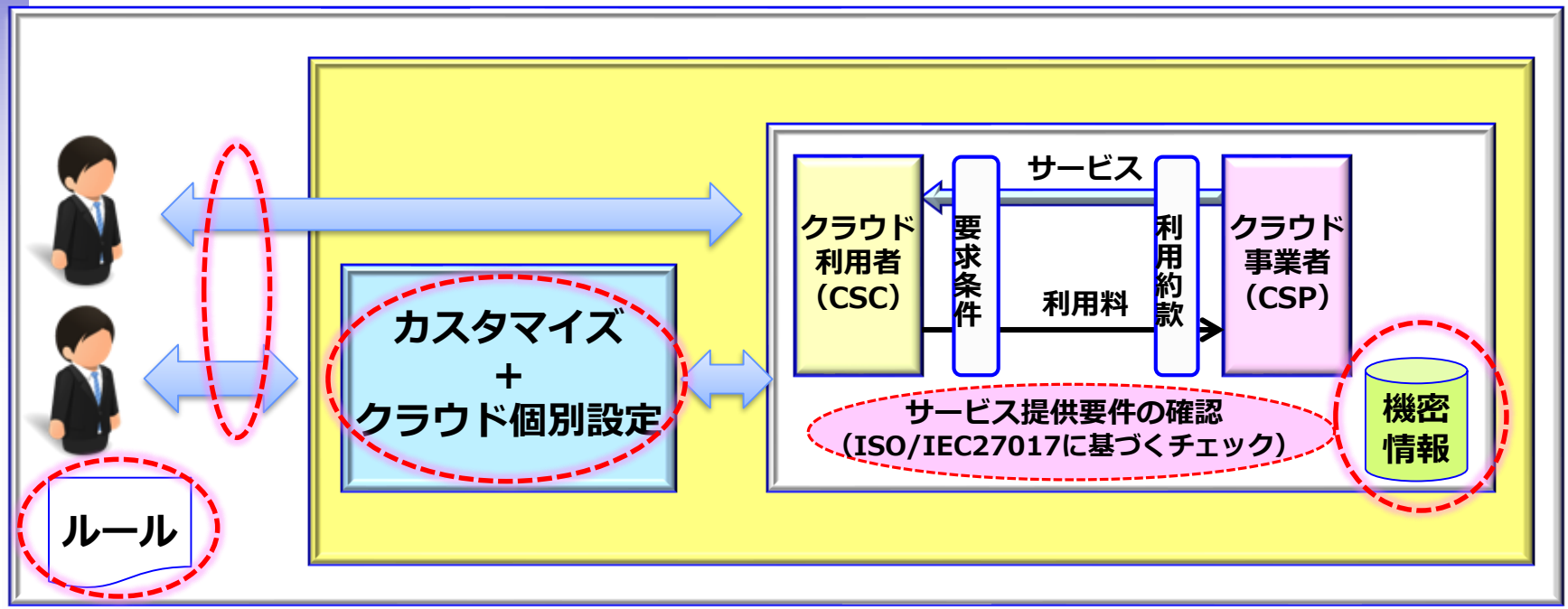
組織として管理（ルール化＆可視化）

- 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



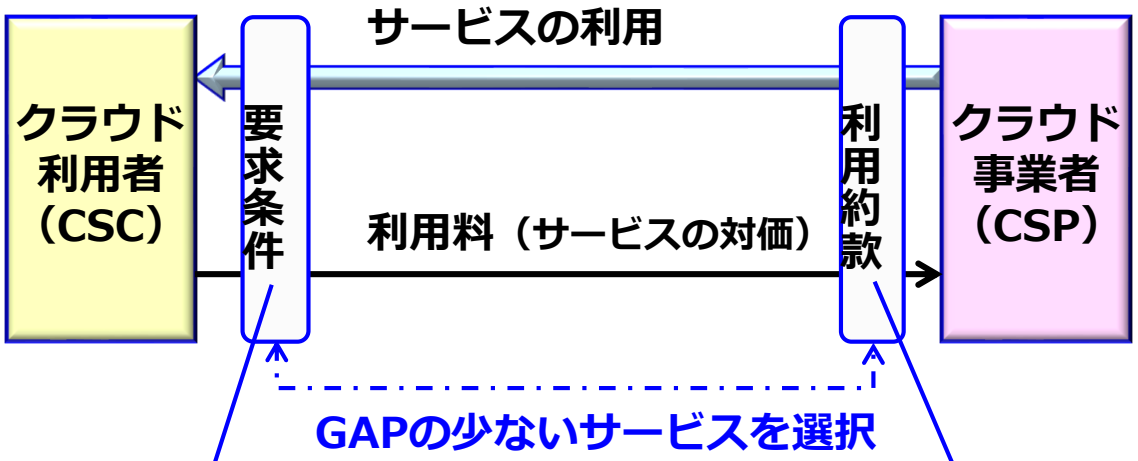
クラウドサービス利用時の確認事項

事例： リスクアセスメントの観点



・どう使うか？
・何に使うか？
・機密情報を保管するのか？
・利用ルールに従うのか？
・誤った使い方？
　（設定誤り、誤操作・・・）

参考：クラウドサービス利用時の確認事項



○機能要件
ｵｰﾄｽｹｰﾘﾝｸﾞ、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/ﾛｸﾞ管理・・
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

まとめ

バランスと協調

クラウド利用

サイバー攻撃対応

協調

ISMS　CSIRT

組織の枠組みを超えて外部とも協調

新たなリスクに対応するためにすべきこと・・・

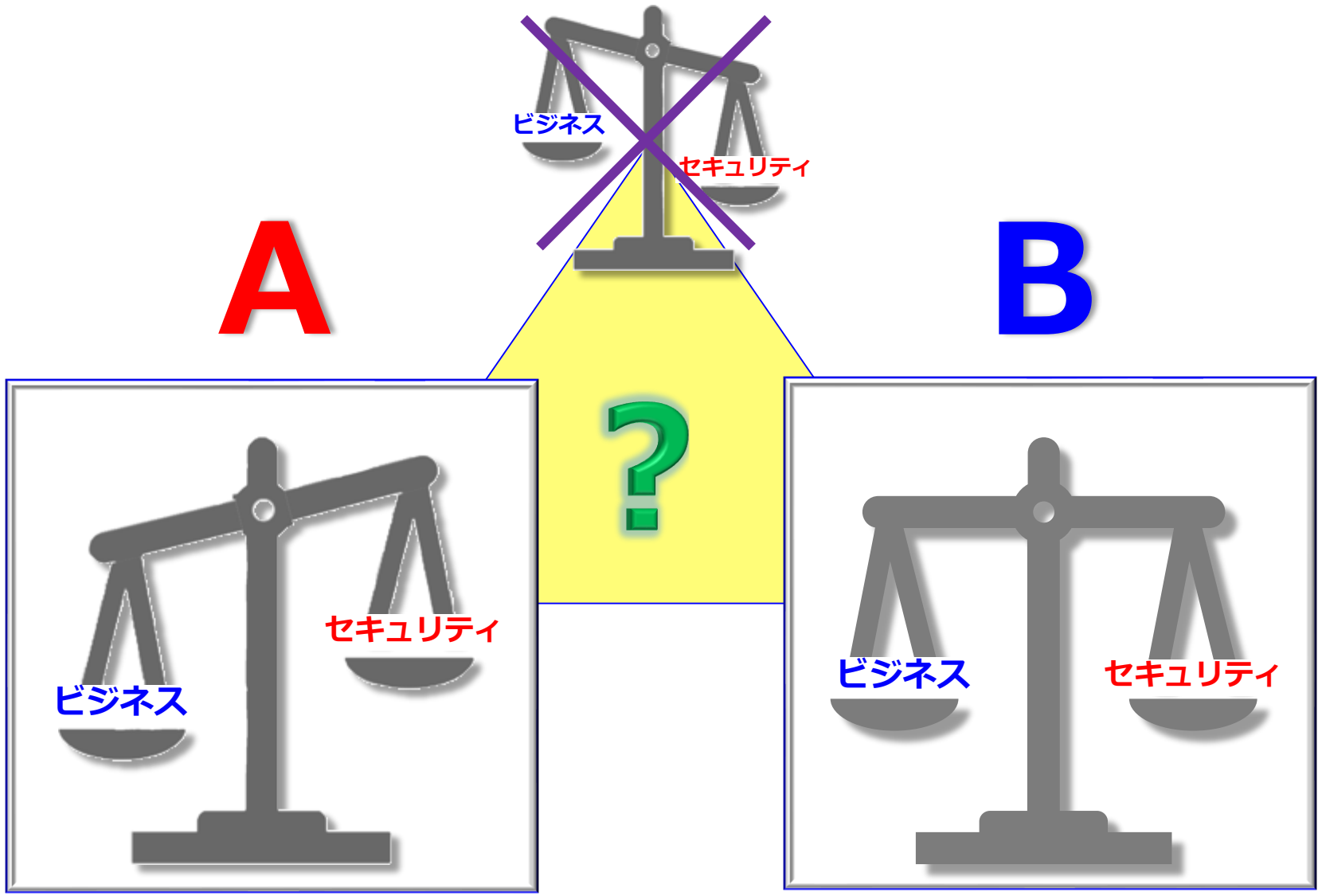
クラウド利用

- クラウドサービスの理解
- リスクの可視化
- 利用ルールの策定
- 野良クラウド排除
- 定期モニタリング

サイバー攻撃対応

- ISMSのスコープとサイバー空間の違いを理解
- 自社の目指すレベル設定
- 受付機能から始める
- CSIRT基本機能の実装・・・

Which do you choose?



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

参加の連絡先は下記まで

主査：masaharu.uowaki@nttcsol.com

ご清聴ありがとうございました。

本日のセミナーでは**最新のビジネス環境リスク（クラウド利用、サイバー攻撃）**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。