JNSA 2023年度活動報告会

日本ISMSユーザグループ

インプリメンテーション研究会活動報告

「 最新の環境の変化に対応したISMSのスコープの再定義など」

標準化部会　日本ISMSユーザグループ
WGリーダー　魚脇 雅晴
（エヌ・ティ・ティ・コミュニケーションズ株式会社）

活動報告内容

1. 日本ISMSユーザグループのご紹介
2. 2022-2023の活動概要（インプリメンテーション研究会）

   -2022年：最新の環境の変化に対応したISMSのスコープの再定義について

   -2023年： ISO/IEC 27001:2022の新規管理策の実装方法についての考察（仮）
3. 2023年の開催イベントのお知らせ

   - 2023年情報セキュリティマネジメントセミナー開催（2023年12月開催予定）
4. インプリメンテーション研究会へのお誘い

日本ISMSユーザグループのご紹介

標準化部会のWG　日本ISMSユーザグループ

業種・業界・分野等の標準化・ガイドライン化などを推進する。
特に、JNSA目線のセキュリティベースラインの提供、情報セキュリティ対策ガイドラインの策定などを進める。また、国際標準/国際連携との親和性の高い案件については、国際標準への提案やコメント、国際連携案件も視野に入れて、議論を進める。さらに、近年のデジタル化促進にともなる技術要素についても積極的に取り上げ、標準化部会での技術共有や課題抽出を実施していく。

・デジタルアイデンティティWG

・電子署名WG

・日本ISMSユーザグループ

・PKI相互運用技術WG

https://www.jnsa.org/active/2023/std.html

日本ISMSユーザグループの活動目的＆予定

１．WGの活動目的

ISMS認証取得企業（ユーザ）とISMSの専門家が連携し、意見交換・議論を進めることで
ISMSの構築・運用に関わるユーザ視点でのベストプラクティスを提供し、日本における
健全かつ効果的なISMS普及・促進に貢献する活動を行う

２．WGの年間活動予定

・インプリメンテーション研究会におけるISMSの構築や運用における課題検討（毎月）
（メインテーマとして「新規格改定に伴う新規管理策の実装方法について」検討を行う）

・情報セキュリティマネジメントセミナーの開催と研究結果の発表（12月）

日本ISMSユーザグループの活動紹介

標準化動向

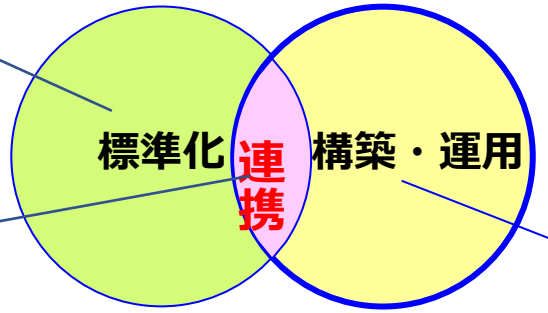
標準化の活用＆定着

ISMSの普及・促進

情報セキュリティセミナー

標準化動向の情報発信

貢献



リエゾン参加

SC 27/WG1 小委員会
アドホック会議

インプリメンテーション研究会

ISMSの構築・運用におけるベストプラクティクスを検討＆提供

標準化されたものをどのように
ビジネスの世界に反映＆定着
させるか・・・

インプリメンテーション研究会の活動紹介

2006年～　ISMSの構築・運用におけるベストプラクティスを検討＆提供　現在

【過去のテーマ名】

2021年
- ■ISMSとゼロトラストセキュリティについての考察
- ■ISMS要求事項の解釈と運用の実態（箇条4について）

2020年
- ■実践かつ効果的なセキュリティ教育
- ■規格の解釈（ISO/IEC27002の改定）に伴う対応についての取り組み

2019年
- ■最新の環境変化に伴うISMSの実装検討
- ■各社の事例から学ぶISMSの実装について

2018年
- ■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

2017年
- ■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

2016年
- ■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

2015年以前は省略

2022年

- ■最新の環境の変化に対応したISMSのスコープの再定義について
- ■続・効率的リスクアセスメント

2023年

- ■ISO/IEC 27001:2022の新規管理策の実装方法についての考察（仮）
- ■続・内部監査（仮）

：本日の活動紹介テーマ（抜粋）

2022年の活動紹介
インプリメンテーション研究会

最新の環境の変化に対応したISMSのスコープの再定義について

（抜粋版）

テーマ選定の理由＆背景と目的

最新の環境の変化に対応したISMSのスコープ（＊1）の再定義について

理由＆背景

従来、オンプレミス（自社所有・自社内設置）中心で構成されたITシステムも近年ではクラウド環境の発達に伴い**クラウド環境へのマイグレーション（移行）が急速**に進んできました。特にスタートアップ企業ではITシステムがすべてクラウド環境だけで構成されているケースも少なくありません 。

また、新型コロナ禍を背景に**リモートワーク・テレワークが増加し、オフィスを縮小**する企業も多くみられるようになりました。

こうした**環境変化は私たちISMS導入組織が従来想定していたリスクをも変化**させているので個々のリスク対策だけではなく、環境全体を見直す必要があるのではないかと考えました。

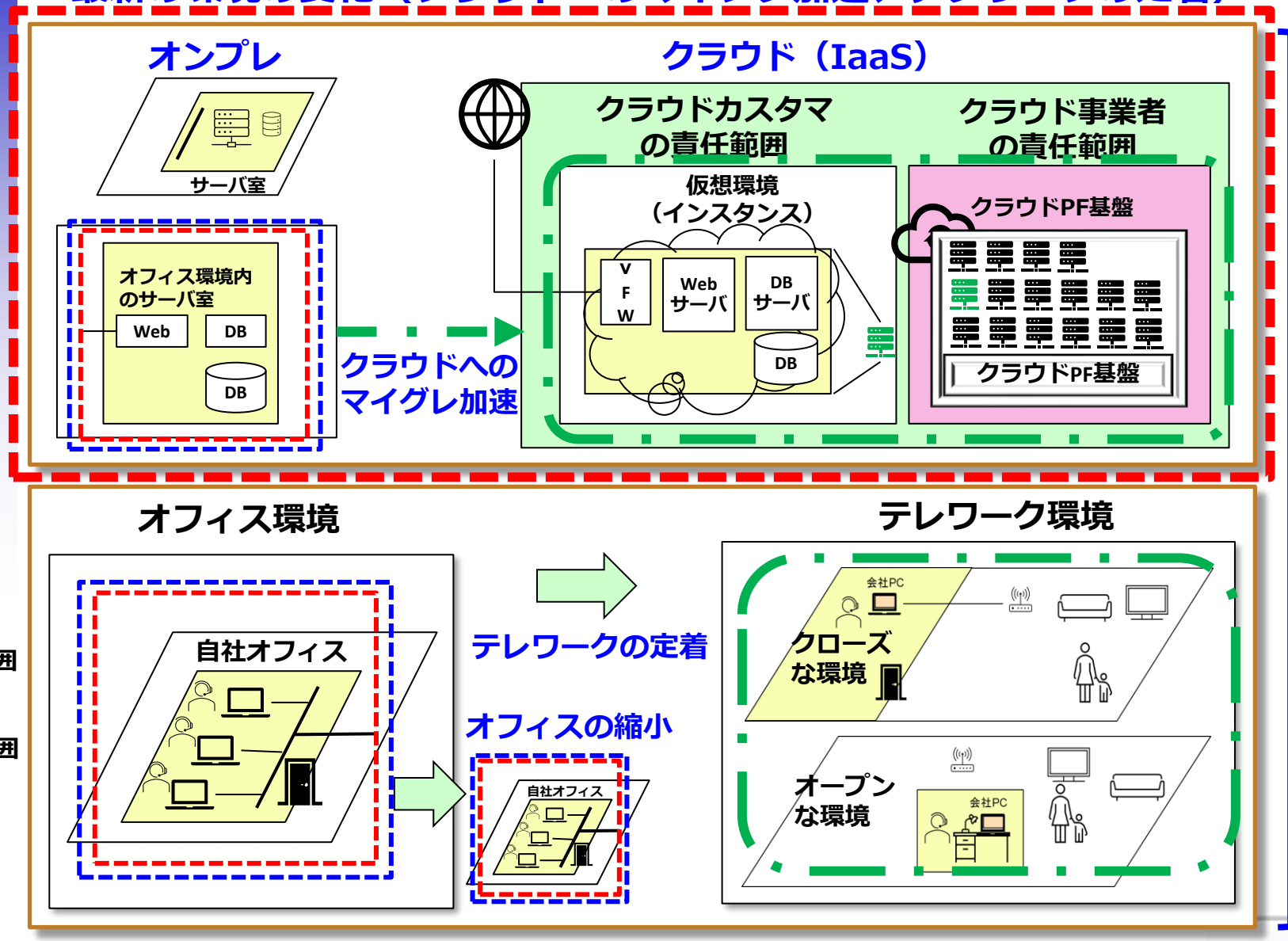
目的

本テーマではこのような**最新の環境の変化（クラウド利用の拡大やテレワークの定着など）を事例としてISMSの適用範囲や認証範囲について規格要求事項の観点から再確認**をすると共に**リスクの変化に対応するための考え方や方針**について整理しました。

＊1：スコープ＝適用範囲

本テーマの狙い　・・・　ポイント2点

最新の環境の変化（クラウドへのマイグレ加速、テレワークの定着）



：適用範囲

：認証範囲

ポイント①

ISMSの適用範囲や認証範囲について規格要求事項の観点から再確認

→適用範囲と認証範囲の変化について可視化

ポイント②

リスクの変化に対応するための考え方や方針を整理

→直接コントロール可能領域と間接コントロール領域について可視化することでセキュリティガバナンスの維持向上を図る

ISMSの適用範囲や認証に関連する規格要求事項について確認

規格要求

規格JISQ 27001の要求事項（箇条4.3）・・・2014年版

規格JISQ 27001の要求事項（2014年版）

4.3 情報セキュリティマネジメントシステムの適用範囲の決定

組織は、ISMSの適用範囲を定めるために、**その境界および適用可能性を決定**しなければならない

この適用範囲を決定するときに、組織は、次の事項を考慮しなければならない

a) 4.1に規定する外部及び内部の課題（組織及びその状況の理解）
b) 4.2に規定する要求事項（利害関係者のニーズ及び期待の理解）
c) 組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係

・2014年の改定時には審査会社から特段の見直しの要求はなかった
・審査工数算出データとなることから整理のためのパラメータとして2006年版の**「事業・組織・所在地・資産・技術の特徴の観点」で整理**をしている。

→規程から具体的な記述は消えているが、包含されたと考えるのが妥当（管理策の分類にも現れている）

新規の認証取得の場合には従来の規程で要求されていることが読み取れない
「境界」をどのような観点で定めるのか基本に戻って規程の要求事項や考え方やフレームワークについて整理したい

認証範囲の申請及び適切性の確認について

（受審組織）

認証範囲の申請

・どのような範囲（組織、部門、業務、プロセス、サービス等）で認証を取得したいのかを定義した文書

「**適用範囲定義書**」

適用範囲を定義した文書

（認証機関）

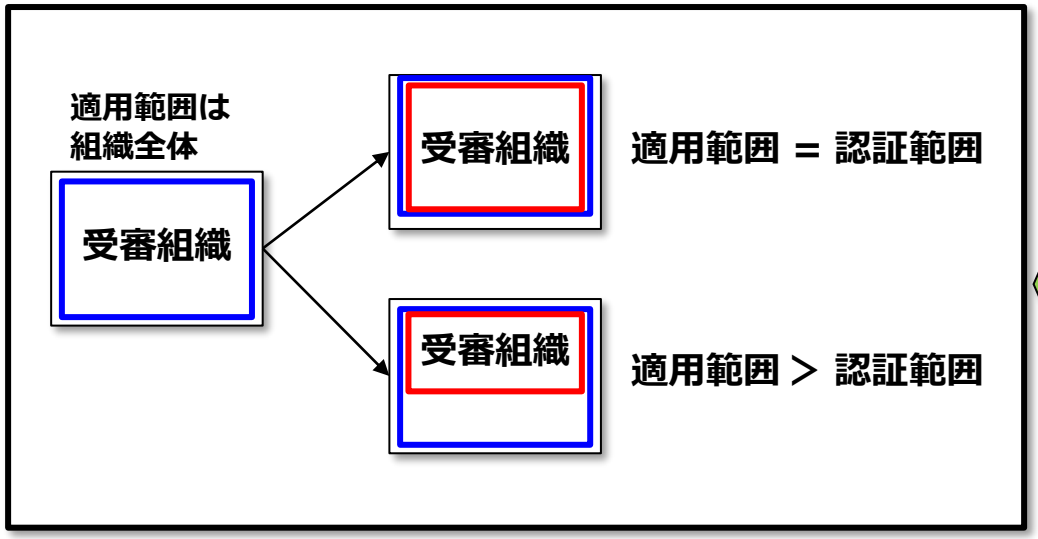
認証範囲の適切性の確認

・本来含めるべき活動を除外している場合、**正当性を評価**
・除外されている規格要求事項がある場合、**正当な理由があり、適切であること**
など

適用規格の取り扱う側面に関連する直接/間接の影響を考慮

適用範囲の決定と認証範囲の明確化の目的

適用範囲の決定と認証範囲の明確化



受審組織の目的

- 自組織で直接コントロール出来る範囲と出来ない範囲を明確化
- 直接コントロール出来ない領域に対するインタフェースを可視化し、間接的にコントロールすることで全体のセキュリティガバナンスを維持・向上できるプロセスを構築する

認証機関の役割

認証の範囲を明確にすることで第三者に認証取得範囲を誤解させない様にコントロールする

副次的な目的

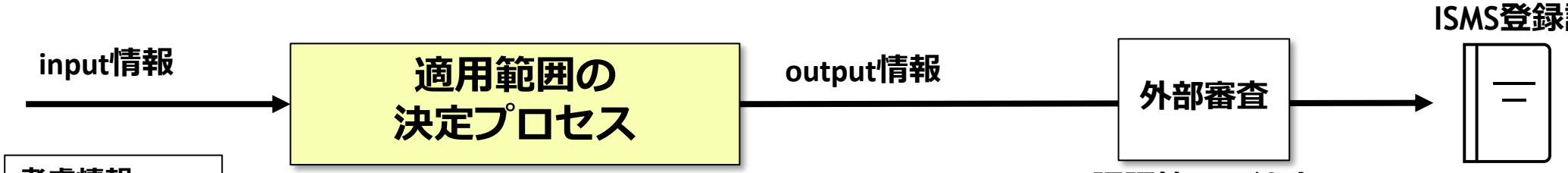
審査に必要なボリューム（稼働）を見積もるためのインプット情報（工数と費用）また、審査員のアサイン時に必要な専門性も可視化できる

：適用範囲

：認証範囲

適用範囲：ISMSのルールが適用される範囲（組織のプロセス、関連サイト、事業部、事業所など）
認証範囲：適合性が証明された認証範囲

適用範囲＆認証範囲の決定プロセス



考慮情報

4.3要求事項の情報

＋

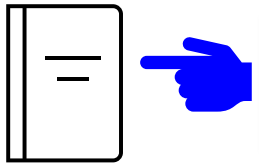
関連情報

- 事業
- 組織
- 所在地
- 資産
- 技術の特徴

- ISMSの適用範囲の仮設定
- 4.3要求事項観点で整理し、適用範囲の妥当性を確認
  - 外部及び内部の課題（組織及びその状況の理解）
  - 要求事項（利害関係者のニーズ及び期待の理解）
  - 組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係
- 直接コントロール出来る範囲と間接コントロールの範囲の可視化
  - 直接と間接の境界ラインについて詳細に検討
  - 必要に応じてリスクアセスメント
- 認証組織内でISMS適用定義書としてまとめる

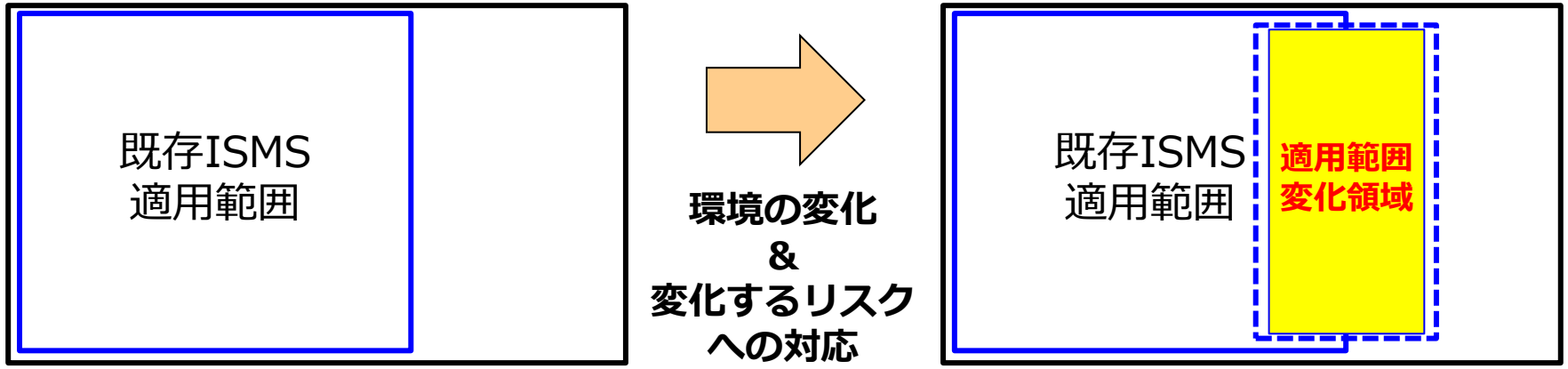
- 審査機関での外部審査を経て認証範囲が正式決定

ISMS適用範囲定義書



認証機関と受審組織との共通認識のためのツールとしても有用である

適用範囲の見直し（再定義）によって変化する項目の可視化



内外の課題の変化

環境の変化（クラウド利用拡大、テレワークの定着）に伴って変化する組織と取り巻く内外の課題

変化するリスク

環境の変化によって発生するリスクに対して自組織で直接コントロール出来る範囲と出来ない範囲を明確化

変化したリスクに対応する管理策

変化したリスクで対応が必要なものに対して管理策として計画＆実施する

適用範囲の見直し

リスク対応を確実なものとするためにISMSの適用範囲の見直し（追加、削除）

事例から紐解く

環境変化

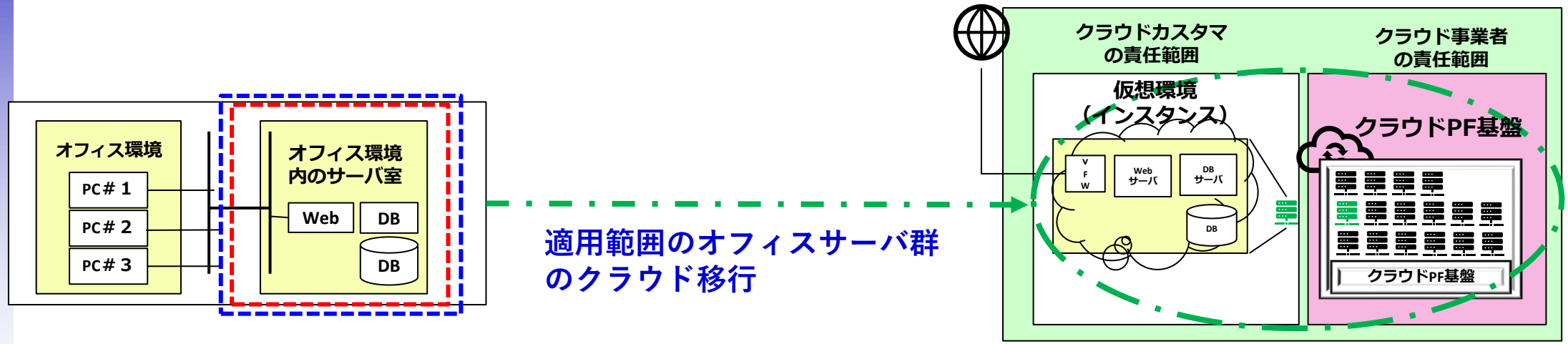
**オンプレからクラウドへの
マイグレーションの加速**

IaaS
事例

環境の変化 （オンプレからクラウドへのマイグレーション）

オンプレ中心のIT環境・・・情報資産は社内NW内に保管

クラウド中心のIT環境・・・情報資産をクラウド上（インスタンス）に保管



：適用範囲

：認証範囲

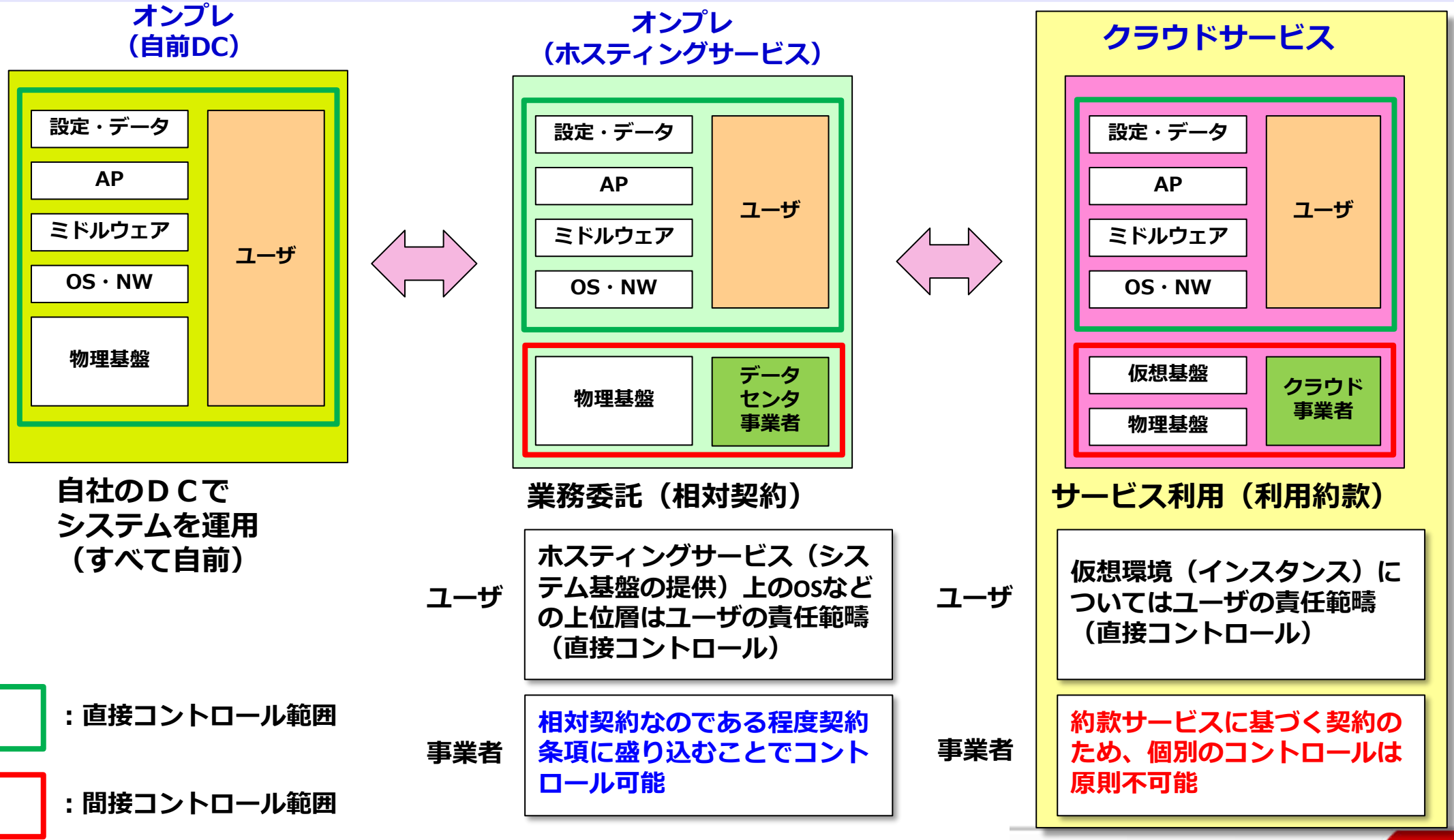
オンプレ

- システム類は社内のサーバルーム
- 固定資産管理として物理資産として管理
- 情報資産は社内エリアに保管
- サーバの保護として物理的管理策

クラウド（仮想環境）

- クラウドの仮想環境（インスタンス）を利用
- 従量制でサービス約款に基づく契約（個別対応不可）
- 情報資産の大半がインターネット上に保管
- 物理よりも技術的な管理策にシフト

サービス契約毎のコントロール範囲の違いについて



自社のＤＣで
システムを運用
（すべて自前）

業務委託（相対契約）

サービス利用（利用約款）

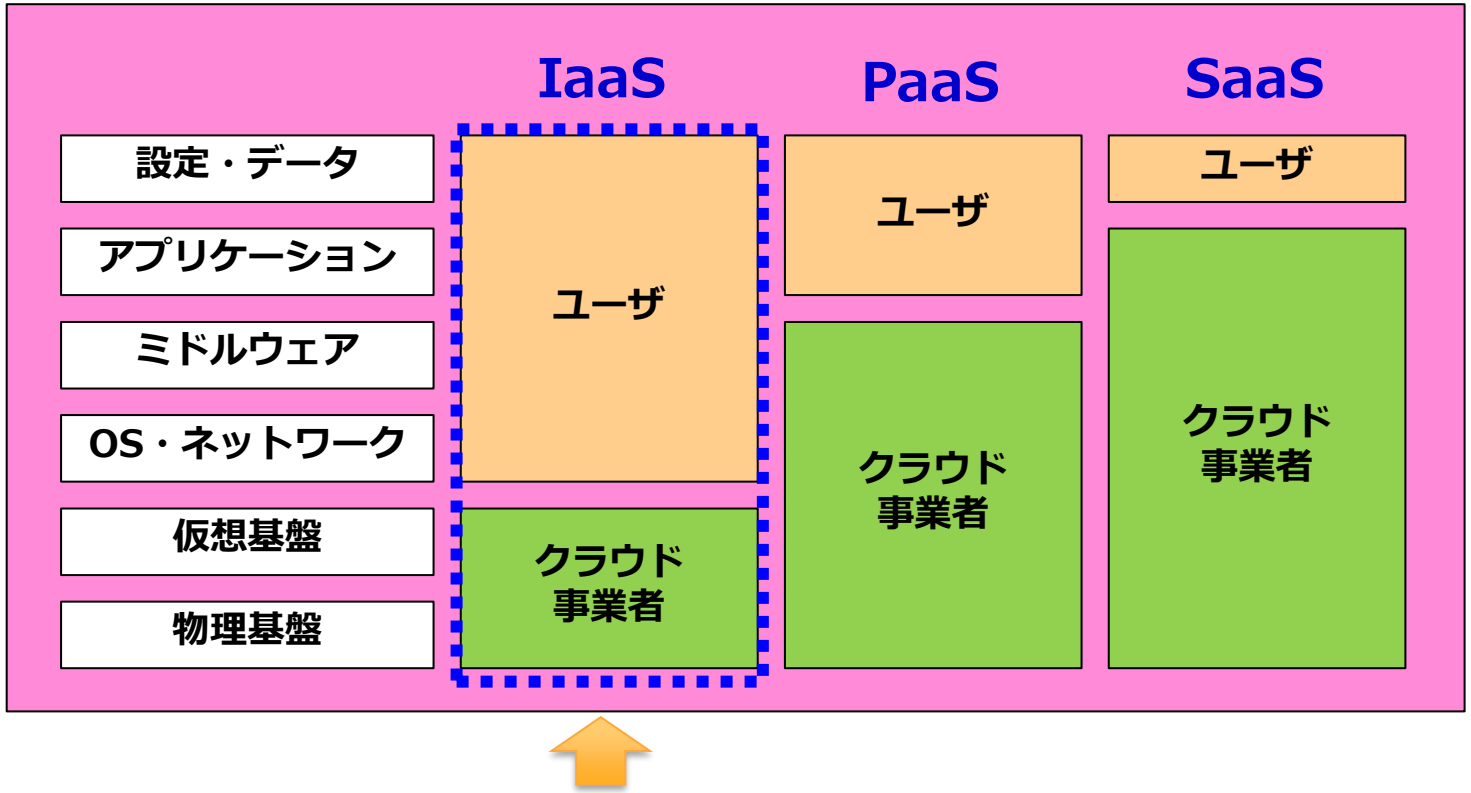
ユーザ	ホスティングサービス（システム基盤の提供）上のOSなどの上位層はユーザの責任範疇（直接コントロール）	ユーザ
		仮想環境（インスタンス）についてはユーザの責任範疇（直接コントロール）
事業者	相対契約なのである程度契約条項に盛り込むことでコントロール可能	事業者
		約款サービスに基づく契約のため、個別のコントロールは原則不可能

：直接コントロール範囲

：間接コントロール範囲

参考： クラウドの責任分界モデル

クラウドサービスの責任分界



責任分界でユーザとクラウド事業者の境界（直接コントロールが可能か否か）が決まる

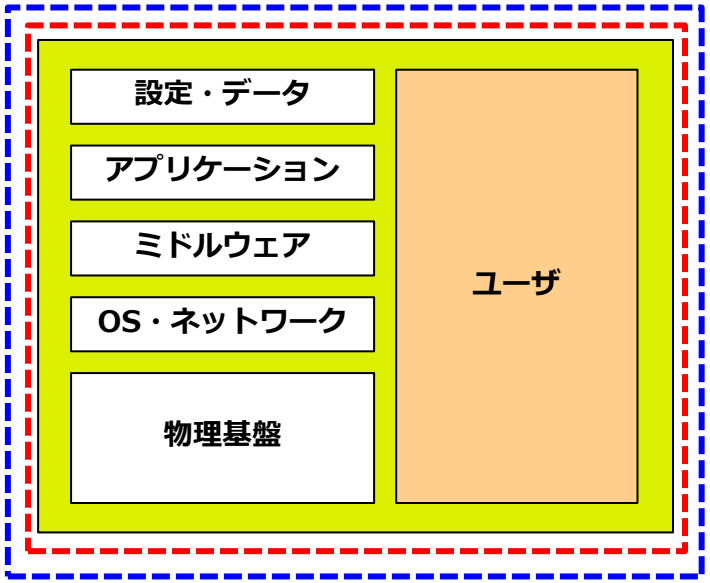
今回の事例で考えるモデル

本パートではIaaSの事例で整理を行う

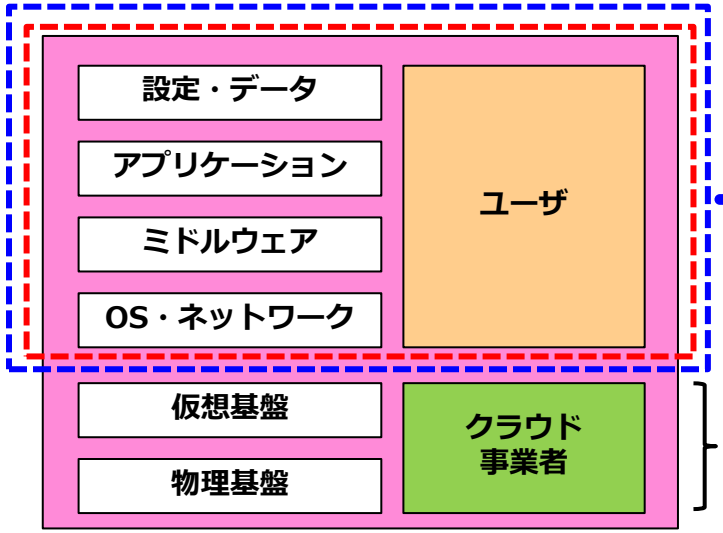
IaaS
事例

環境の変化 （オンプレからクラウドへのマイグレーション）

オンプレの責任範囲



クラウドサービスの責任分界（IaaS)



クラウドサービスの責任分界からユーザの責任範囲であること&ユーザとして直接コントロールが可能であることからISMSの適用範囲＆認証範囲とする

A15　の供給者関係での整理事項

従来のオンプレからクラウドサービス（仮想環境）に移行

①適用範囲、認証範囲は仮想環境上のシステム

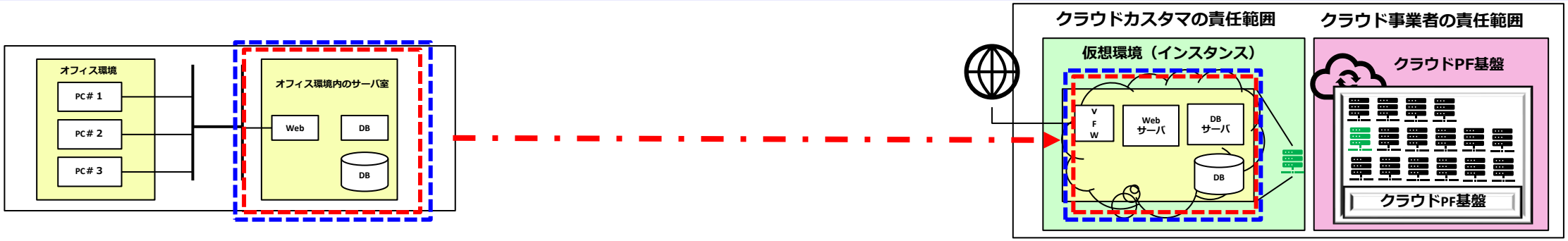
②クラウドPF基盤については利用者としては直接コントロール出来ないため、A15 供給者の関係で整理する

：適用範囲

：認証範囲

IaaS
事例

クラウドマイグレのユーザコントロール範囲内、範囲外



分類	構成要素	補足説明
データ	保有データ	社内NW内に保有
物理構成	DBサーバ	ラック内
	Webサーバ	同上
	FW	同上
	NW	同上
インフラ	ラック	施錠管理
	空調	個別空調
	電力	法廷点検時は停止
	物理エリア	施錠管理

分類	構成要素	補足説明	ユーザコントロール範囲
データ	保有データ	クラウド内仮想環境（インスタンス）	範囲内
仮想構成	DBサーバ	クラウド内仮想環境（インスタンス）	範囲内（割り当てられたインスタンスの範囲内で自由に利用可能）
	Webサーバ	同上	
	FW	同上	
	NW	同上	
クラウドPF基盤	DBサーバ	クラウドPF基盤構成要素	**範囲外（クラウドサービス約款の中で稼働率などの契約の数値として現れるが、相対契約のような調整の余地はない）**
	Webサーバ	同上	
	FW	同上	
	NW	同上	
	ラック	同上	
	空調	同上	
	電力	同上	
	物理エリア	同上	

：適用範囲

：認証範囲

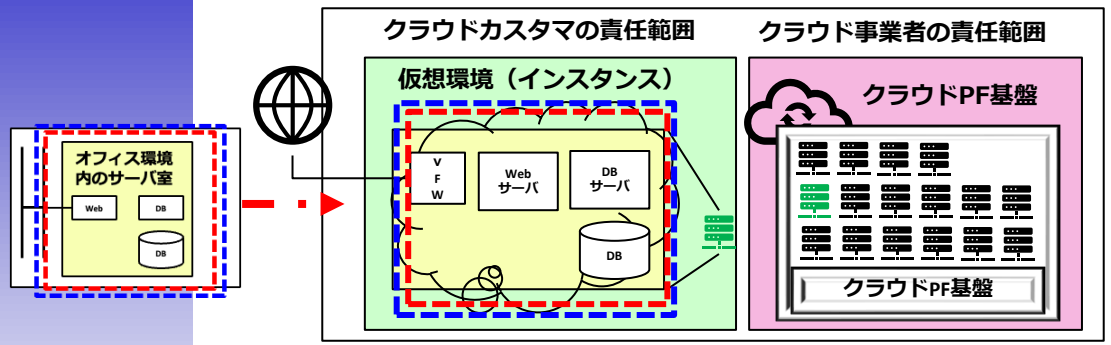
環境の変化（クラウドシフト）に関する考慮事項（箇条4.3）

項目	要求される対応項目	対応方針	備考
外部の課題	**法令やガイドラインへの対応** ・情報資産に含まれる個人情報の保管先についての確認（リージョンが国内か国外か？） ・個人情報保護法/ガイドラインなどの遵法性	**クラウドサービス選定時に約款を確認**することで**国内リージョンの選択が可能か否かを選定条件**とする **係争等の裁判時のどの国の法律に準ずるか、どこの管轄の裁判所（合意管轄）か事前に確認することが重要** また、個人情報の取り扱いがある場合には法規制やガイドラインの準拠性も確認する	間接コントロール
	サイバー攻撃への対応 ・インターネットに情報資産が保管されることでより外部からの攻撃のリスクが増加 ・SaaS利用によるインターネット上での情報資産の保管の増加、管理外の利用の増加	サイバー攻撃のリスクが高くなることから、旧来のオンプレの時のリスクアセスメントでは不十分なので**新たにリスクアセスメントを実施し、追加の管理策を実施**する **侵入前提の対応策の検討**（ゼロトラストセキュリティの考え方の導入含めて）	直接コントロール SaaSは間接コントロール
内部の課題	**情報セキュリティに関する体制やルールの整備** ・クラウド利用に関する社内ガイドラインの整備	クラウド利用における**社内ガイドライン（利用ルール）の策定＆教育＆周知の徹底**	直接コントロール
	従業者のセキュリティリテラシーの向上 ・無許可のクラウド（野良クラウド利用防止）利用禁止の遵守	社内のクラウド利用のガイドラインに従った安心、安全なクラウドを利用登録して利用することを**従業員全員に研修＆理解**させる	直接コントロール

環境の変化（クラウドシフト）に関する考慮事項（箇条4.3）

項目	要求される対応項目	対応方針	備考
利害関係者のニーズ及び期待の理解	**預託した機密情報がインターネット上において適切に管理**されている（預託した個人情報がある場合も含めて）	外部の課題とも関連するが、利用を想定しているクラウドのリージョンが**国内に限定できることを事前に確認**する（**約款の確認**が必要） また、**契約時に確実に履行出来ることも確認**する ・個人情報保護法などの遵法性の確認 ・不正アクセスされた場合に検知＆初動対応が可能となる管理策の追加（モニタリング）	
組織が実施する活動と他の組織が実施する活動との間のインフェース及び依存関係	クラウドサービスを利用することで、**クラウドサービス事業者（CSP）とクラウドサービスカスタマ（CSC）との関係**に移行する（直接コントロール出来る範囲が限定される）	**クラウドの責任分界モデルやA.15供給者との関係で整理**を行う また、加えて**コントロール内、コントロール外での管理策の考えに基づき整理を行い、必要に応じて追加の管理策の検討**を行う **ISO27017クラウドサービスのための情報セキュリティ管理策に基づきCSC（クラウドサービスカスタマ）の立場での要件の確認** **→独自に自社で調査を行い、管理方針を策定（要求条件の可視化＆GAP分析）** **→ISMAPを利用した要件の確認**	

適用範囲見直しにおける考慮ポイント・・・クラウドへのマイグレ加速



→ 単純にリアルマシンから仮想マシンへの移行だけでない！

→ 右記に示す箇条4.3の要求事項を考慮した検討プロセスが必要

＋α

箇条4.3の要求事項の考慮ポイント

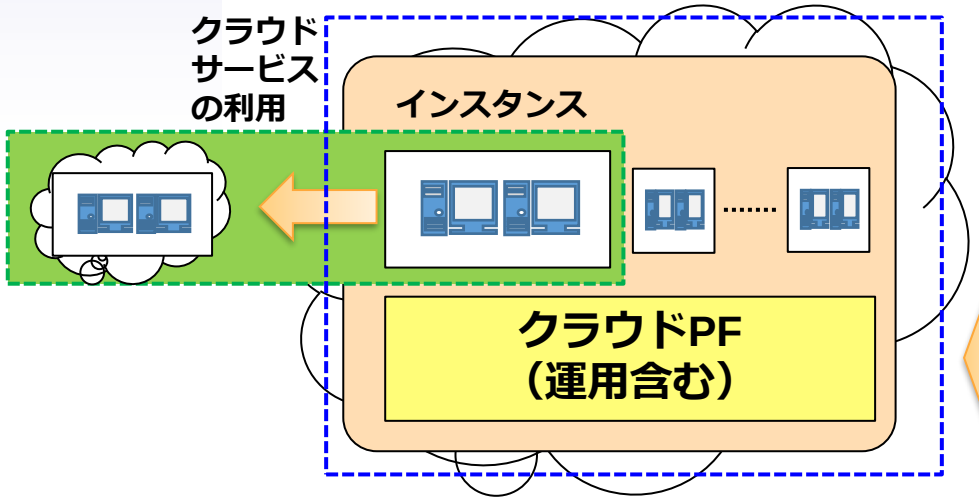
○外部の課題
　法令やガイドラインへの対応
　（約款の確認、国内リージョン指定など）
○内部の課題
　クラウド利用のガイドラインの制定＆教育
　従業員研修
○利害関係者のニーズ及び期待の理解
　インターネット上でシステムや機密情報が
　適切に管理運用されていること
○組織が実施する活動と他の組織が実施する活動
　との間のインフェース及び依存関係
　クラウド責任分解モデルやA15供給者との関係で整理
　コントロール内、コントロール外での管理策の考えに
　基づき整理を行い、必要に応じて追加の管理策の検討
　→ISMAPを利用した要件の確認（次ページ参照）

参考：ISMAPとは？

政府情報システムのためのセキュリティ評価制度
（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））

政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスの円滑な導入に資することを目的とした制度です。

CSP（クラウドサービスプロバイダー）
（クラウドを社会インフラ基盤として提供）



ISMAPによる安心・安全なクラウドサービスの確保

ISMAPクラウドサービスリストに登録するためには、下記の要求事項、管理基準を満たす必要がある

- **クラウドサービス登録申請者に対する要求事項**
- **情報セキュリティ管理・運用の基準となる管理基準**
- **監査機関登録申請者に対する要求事項**

まとめ（振り返り）

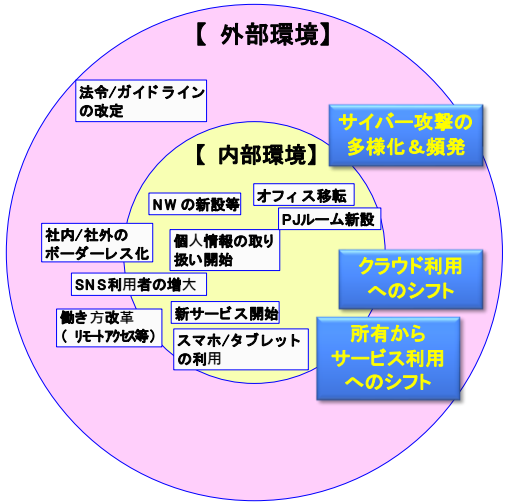
- 基本に帰る（規格要求事項）

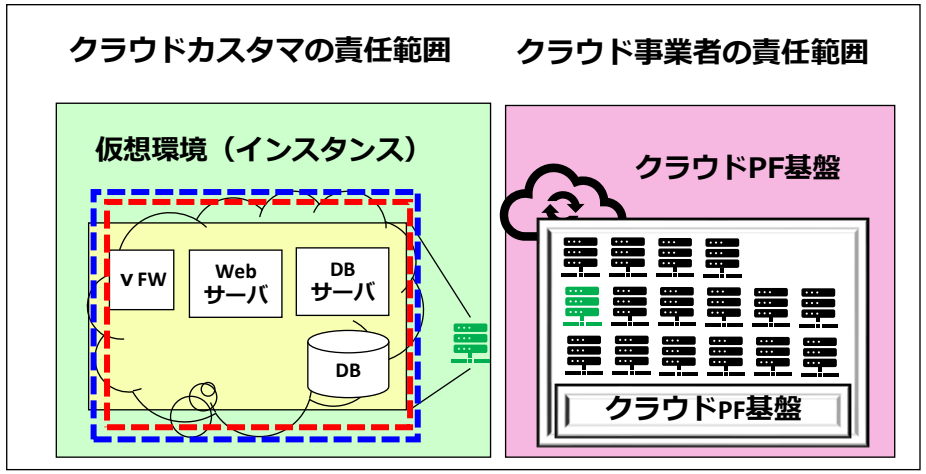
4.3 情報セキュリティマネジメントシステムの適用範囲の決定

～、　**その境界および適用可能性を決定**　～
この適用範囲を決定するときに、組織は、次の事項を考慮　～

a) 4.1に規定する外部及び内部の課題（組織及びその状況の理解）
b) 4.2に規定する要求事項（利害関係者のニーズ及び期待の理解）
c) 組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係

- 環境の変化に敏感になる
- リスクの変化
  →コントロール内／外
  →的確にリスク対応を行う

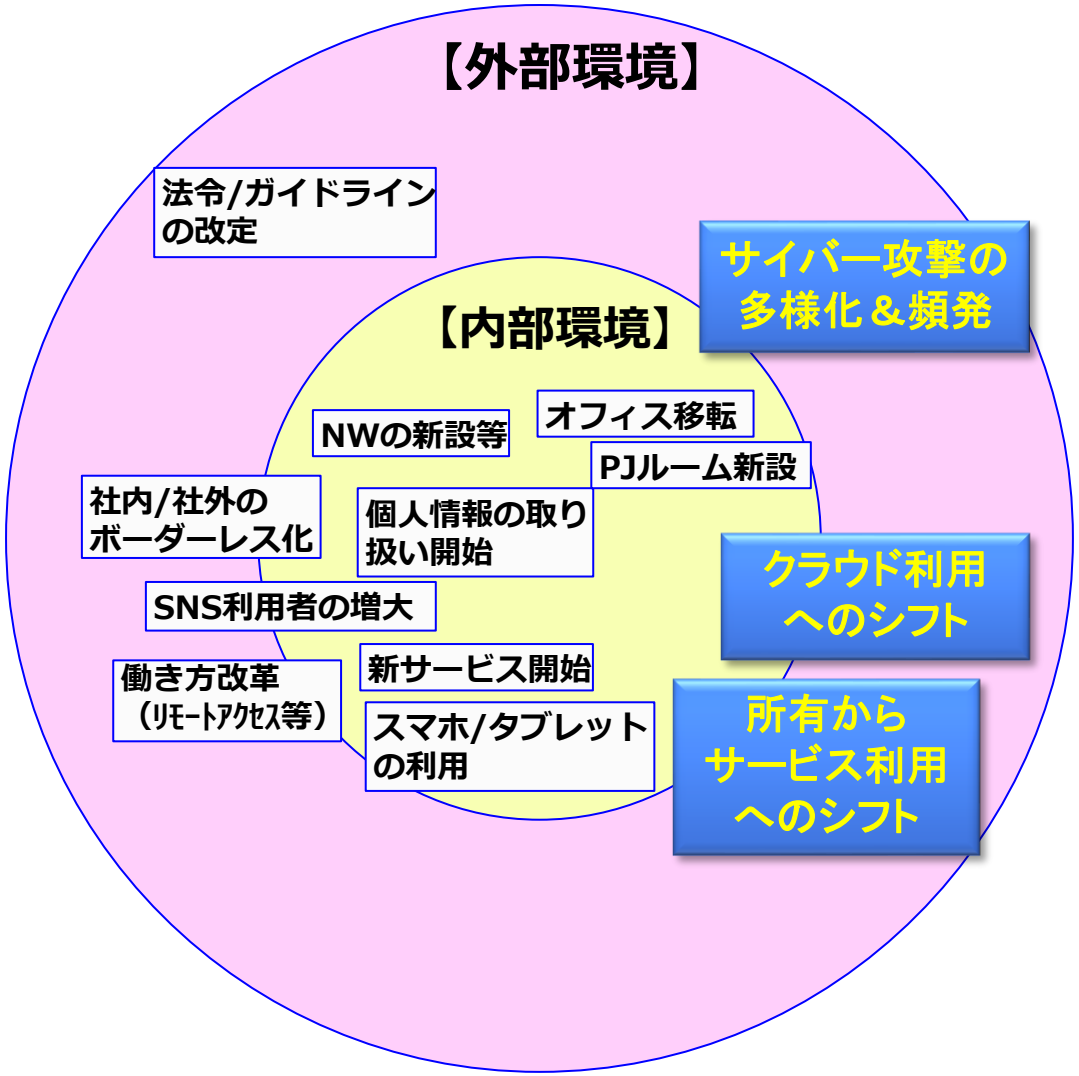




直接コントロール　　**間接コントロール**

参考

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	・・・

■情報セキュリティマネジメントセミナー2022

（27000シリーズの最新動向とベストプラクティスの提案）　2022.12.16開催

JNSA

標準化動向とベストプラクティスのご紹介

【標準化動向】

- ISO/IEC 27001改定内容と関連規格の動向
- ISO/IEC 27002改定の解説

【研究会成果報告】

- 最新の環境の変化に対応したISMSのスコープの再定義について
- 続・効率的リスクアセスメント

【パネルディスカッション】

- ISO/IEC 27002, 及び27001の改訂に伴う課題や今後の必要な対応

毎年12月にまとめとして情報セキュリティセミナーを開催しています

本日、ご紹介したテーマ

参考：2022年セミナー開催情報＆講演資料

https://www.jnsa.org/seminar/2022/isms2022/index.html

ご紹介したテーマの資料のフルセットはココに掲載しています

2023年の活動紹介

・インプリメンテーション研究会

ISO/IEC 27001:2022の新規管理策の実装方法についての考察（仮）

続・内部監査（仮）

・情報セキュリティマネジメントセミナー2023（12月開催予告）

テーマとして選んだ背景

ISO/IEC27001が2022年10月に改訂された

JIS化を予定されているが少し遅れている

認証組織ではJISQ27001：2015からJISQ27001：2023への移行が大きなイベントとして予定されている

新規の管理策が11個あるので要求事項を正しく理解した実装が必要

ISO/IEC 27001:2022の新規管理策の実装方法についての考察（仮）

抜粋版

	テーマ名	テーマの活動概要	備考
テーマ1	ISO/IEC 27001:2022の新規管理策の実装方法についての考察(仮題)	規格改定された要求事項の中で今回追加された新規の管理策11個についてどのように実装すればよいか整理を行うことで各認証組織が新規格への移行検討において参考に出来るアウトプットとしてまとめる（下記の方向性で） ・新規格の要求事項の明確化 ・組織の成熟度に応じた対応方針（松竹梅） ・具体的な実装事例の提示 ・疑問点は残さない（・・・出来るだけ）	
テーマ2	マンネリ化や内部監査など過去のテーマ（課題）	マンネリ化や内部監査など過去のテーマについて取り巻く環境や研究会メンバーも代わっているので再整理することで新しい発見が生まれる可能性がある	

ISO/IEC 27001:2022の新規管理策の実装方法についての考察（仮）

抜粋版

ISO/IEC 27001:2022, Annex Aの新規管理策（11個）

本日は抜粋版で
頭出しでご紹介

	新規管理策
1	**5.7 脅威インテリジェンス**
2	5.23 クラウドサービス利用における情報セキュリティ
3	5.30 事業継続のための ICT の備え
4	7.4 物理的セキュリティの監視
5	**8.9 構成管理**
6	8.10 情報の削除
7	8.11 データマスキング
8	8.12 データ漏えいの防止
9	**8.16 監視活動**
10	8.23 ウェブフィルタリング
11	8.28 セキュリティに配慮したコーディング

ISMSの規格要求事項から実装要件の整理

新規管理策の実装における指針や考え方についての提案

実装についてはベストプラクティスではなく松竹梅などのレベルに応じたものを提案したい

5.7 脅威インテリジェンス（要約）

抜粋版

概要

脅威に関する情報を収集及び分析し、脅威に対する対策を講じることで、組織のISMSに影響を及ぼすリスクを低減するための活動に繋げる

目的

サイバーセキュリティの脅威（※1）から組織の活動を守るため

※1：このテーマの中では、人的、組織的、物理的、技術的の4つの分野の脅威の中から、変化が激しく組織に重大な影響を与える可能性の高いサイバーセキュリティの脅威を「脅威インテリジェンス」の研究対象とする

誰がどのように活用するのか？

・経営戦略的な判断をするための入力情報として活用（経営層）

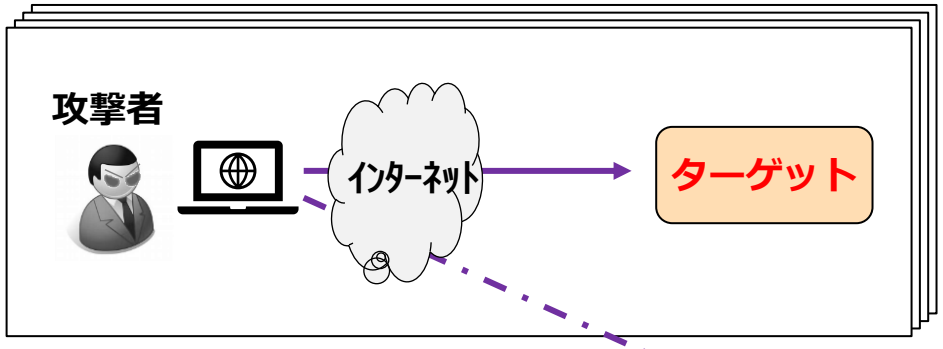
・予想される攻撃や実際の攻撃から防御するための入力情報として活用
（セキュリティの専門家、システム担当など）

＜情報の例示＞
サイバーセキュリティの専門家が分析・整理したサイバー攻撃に関する情報

・攻撃のメカニズム（攻撃手法）
・攻撃の発生の識別方法
・攻撃によってビジネスに与える影響
・防御方法などのアドバイス
・攻撃を実現させる環境・条件があるか

脅威インテリジェンスとは？（イメージ図）

抜粋版



サイバーセキュリティの
専門家が分析・整理した
サイバー攻撃に関する
情報を収集

外部組織

専門組織

セキュリティ研究機関、
NPO法人、セキュリティティ
ベンダー、など

サイバー攻撃に関する情報

- 攻撃のメカニズム（攻撃手法）
- 攻撃の発生の識別方法
- 攻撃によってビジネスに与える影響
- 防御方法などのアドバイス

内部組織

防御

戦略情報として
のインプット

マネジメント層
主要な意思決定者、
CEO、取締役など

セキュリティ担当
セキュリティ技術者
CSIRTやISMS事務局

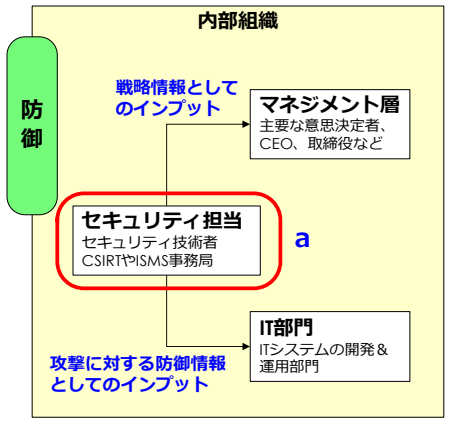
IT部門
ITシステムの開発＆
運用部門

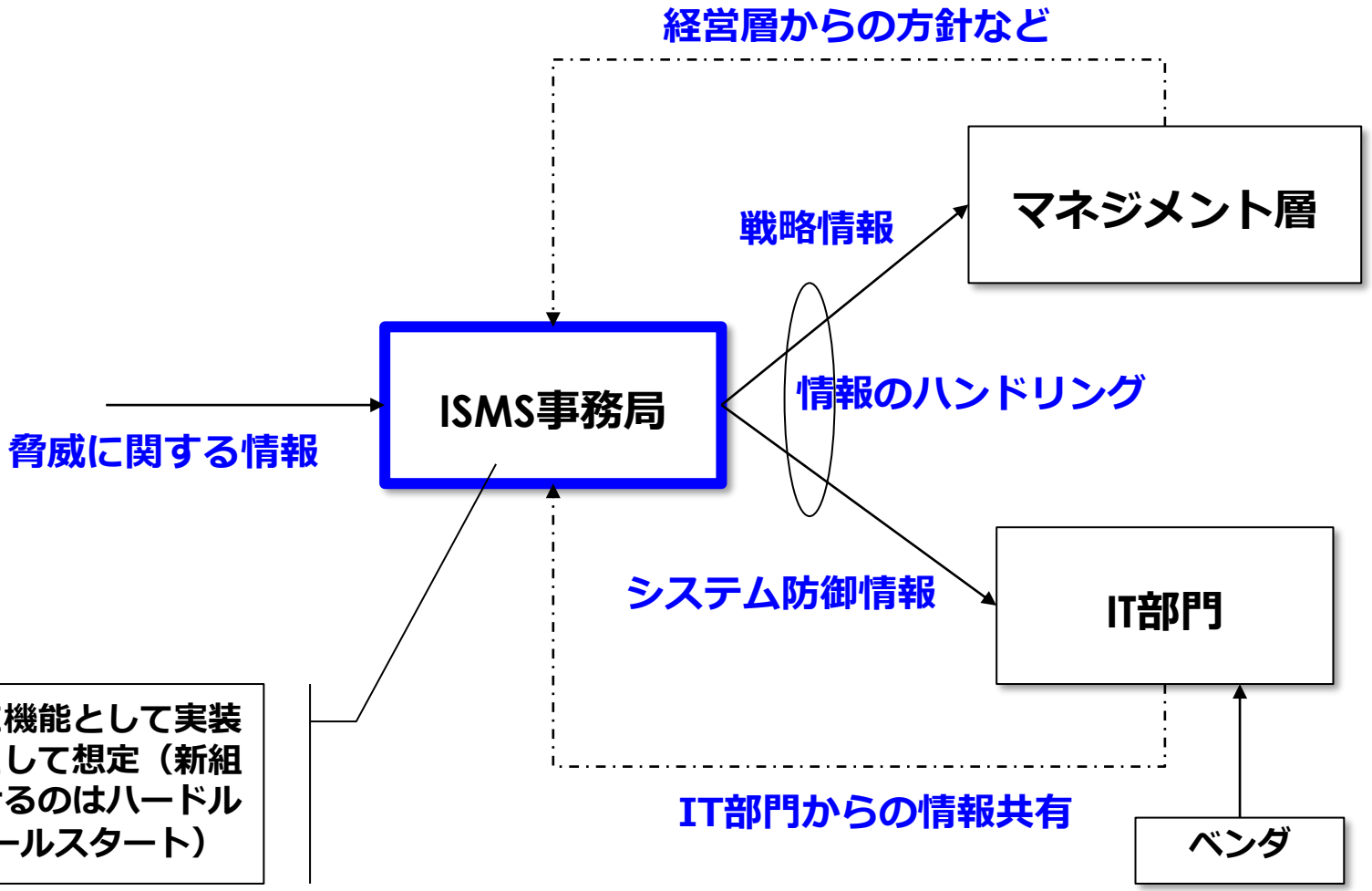
攻撃に対する防御情報
としてのインプット

セキュリティ担当（a）の役割

抜粋版

a.脅威情報を簡易分析（判断）する機能を実装し、情報をハンドリング



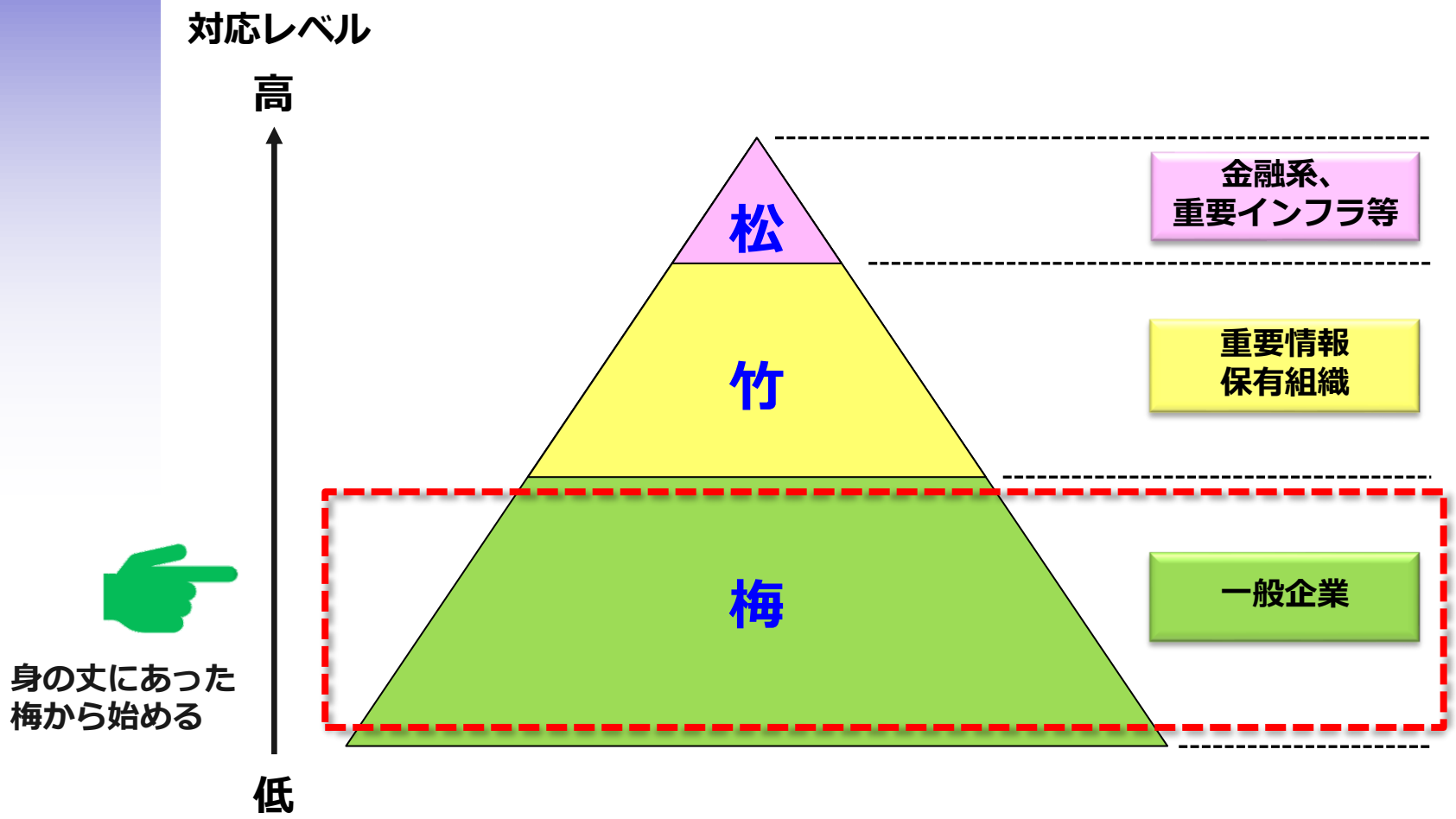


既存の組織の中に機能として実装することを前提として想定（新組織として独立させるのはハードルが高いのでスモールスタート）

脅威インテリジェンスの対応レベルについての考え方（案）

抜粋版

組織特性毎の脅威インテリジェンスの要求レベル（案）



管理レベル

CSIRT体制を確立し、
脅威インテリジェンスの活用
を徹底しなければならない

CSIRT体制を確立し、
脅威インテリジェンスの活用
のプロセスを構築＆運用
しなければならない

- ISMSは取得済み
- CSIRT体制構築の
  余裕無し
- 最低限の機能実装を行い
  脅威インテリジェンス
  を活用しなければならない

この続きは情報セキュリティマネジメントセミナー2023にて・・・

ISO/IEC 27001:2022, Annex Aの新規管理策（11個）

	新規管理策
1	**5.7 脅威インテリジェンス**
2	5.23 クラウドサービス利用における情報セキュリティ
3	5.30 事業継続のための ICT の備え
4	7.4 物理的セキュリティの監視
5	**8.9 構成管理**
6	8.10 情報の削除
7	8.11 データマスキング
8	8.12 データ漏えいの防止
9	**8.16 監視活動**
10	8.23 ウェブフィルタリング
11	8.28 セキュリティに配慮したコーディング

情報セキュリティマネジメントセミナー2023にてインプリメンテーション研究会の成果として発表予定です

新規管理策の実装における指針や考え方についての提案

■情報セキュリティマネジメントセミナー2023

（27000シリーズの最新動向とベストプラクティスの提案）

開催予告

JNSA

2023年12月○○日（○）午後　・・・　日程は別途、案内予定

【標準化動向】

ISO27001、ISO27002などの27000シリーズの標準化の最新動向など

【研究会成果報告】

インプリメンテーション研究会の活動成果

・テーマ1：ISO/IEC 27001:2022の新規管理策の実装方法についての考察（仮）
・テーマ2：続・内部監査（仮）

【パネルディスカッション】

最新のトピックについてディスカッション予定（仮）

■インプリメンテーション研究会へのお誘い

毎年、**組織を取り巻く環境の変化に対応したテーマに挑戦**して ISMSの構築・運用における
ベストプラクティクスを検討しています。
ご興味のある方は一緒に検討に参加頂ければ幸いです。
冷やかしも大歓迎ですので、気軽にJNSA事務局へご連絡ください。

テーマ1:　**ISO/IEC 27001:2022の新規管理策の実装方法についての考察（仮）**

テーマ2:　続・内部監査（仮）

現在、ハイブリッド（Web会議＋
リアル会場）で討議しています！
毎月最終木曜日18:00～21:00