Japan Information Security
Management Systems User Group

講演３

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

JNSA 標準化部会

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

2022年12月16日

魚脇　雅晴

（エヌ・ティ・ティ・コミュニケーションズ株式会社）

日本ISMSユーザグループの活動紹介

標準化動向

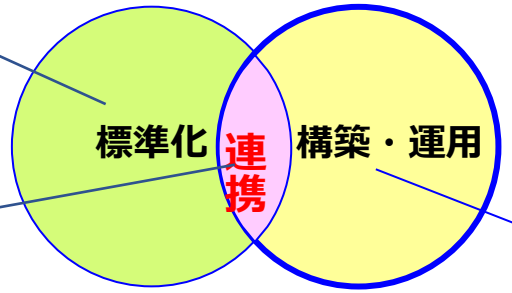
標準化の活用＆定着

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～　　現在

ISMSの構築・運用におけるベストプラクティスを検討＆提供

【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（講演3）

■続・効率的リスクアセスメント（講演4）

：本日の発表テーマ

テーマ選定理由＆テーマ概要

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

【概要】

本テーマでは最新の環境の変化に対応したISMSのスコープ＊1について再考を行います。

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。

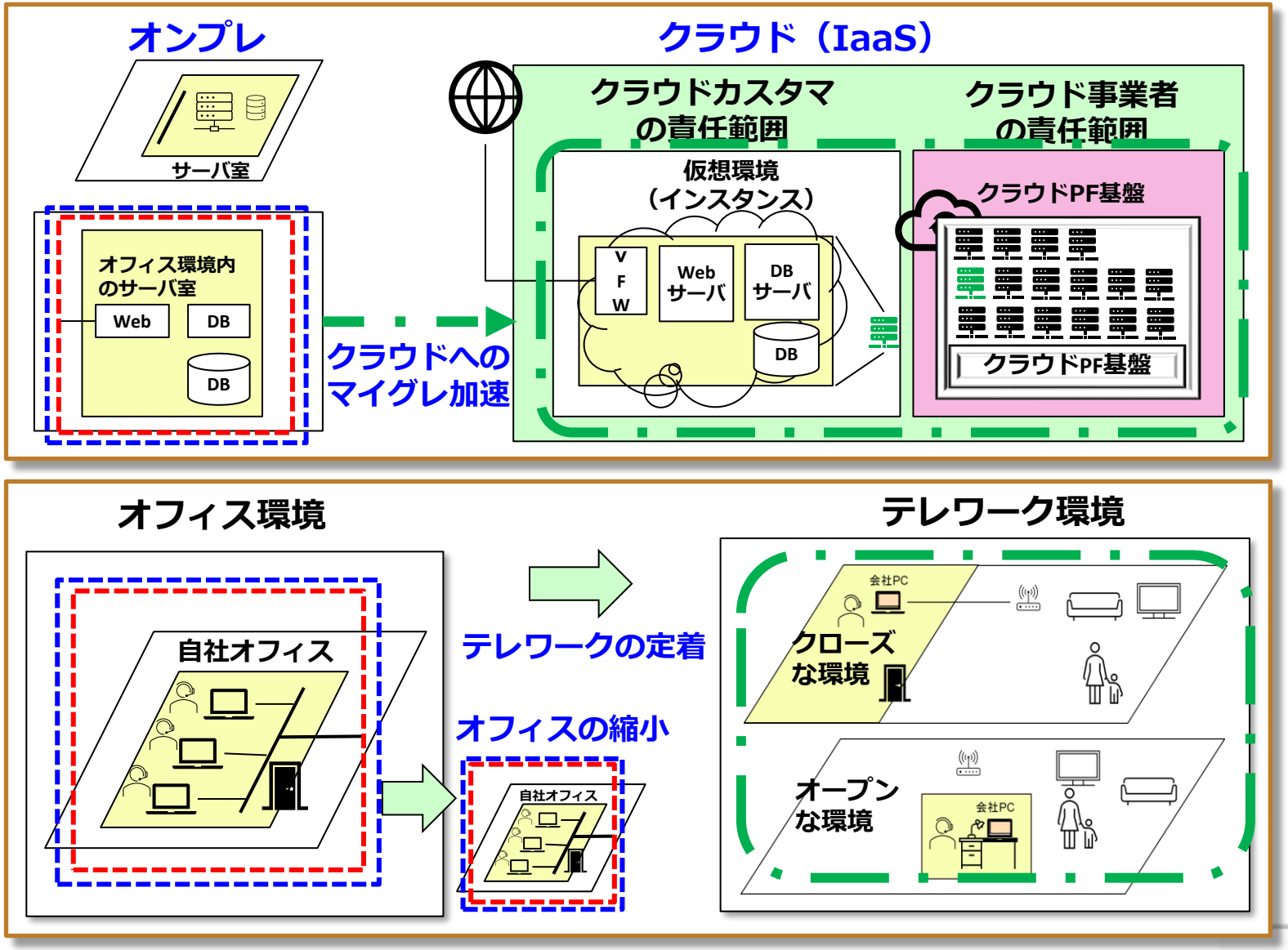
こうした変化は私たちISMS導入組織が従来想定していたリスクをも変化させているので個々のリスク対策だけではなく、環境全体を見直す必要があるのではないかと考えました。

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

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

最新の環境の変化を事例にして下記の整理を行う

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

参考：　【国際認証の組織と規格の関連】

IAF＊1

認証機関の認定に係る国際的専門機関

認定基準に適合していることを証明して貰うか信任して
もらう事で、国別の認証制度の相互承認が受けられる

IAFの認定基準は、JIS Q 17011:2018適合性評価―適合性評価機関の認定を行う機関に対する要求事項

認定機関

第三者審査 認証 を採用する規格において
審査機関を認定する組織

IAFが認定又は信任した機関（日本では、ISMS-ACとJAB）
で、認証機関（審査機関とも言う）を認定する

JIS Q 17021-1:2015適合性評価―マネジメントシステムの審査及び認証を行う機関に対する要求事項―第１部：要求事項
JIS Q 27006:2018情報技術–セキュリティ技術– 情報セキュリティマネジメントシステムの審査及び認証を行う機関に対する要求事項

認証機関

ISO、IEC、ISO/IEC認証の取得を希望
する企業や団体を審査する機関

認定を受けた認証機関は、認証基準に基づく審査を実施し
認証授与を決定する

JIS Q 27001:2014情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項

受審組織

ISO、IEC、ISO/IEC認証の取得を希望
する企業や団体

＊1：IAF(International Accreditation Forum, Inc. 国際認定フォーラム)

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

規格要求

JIS Q 17021-1：2015の要求事項（認証機関に対する要求事項）

適合性評価–マネジメントシステムの審査及び認証を行う機関に対する要求事項–第1部：要求事項

9.4 審査の実施
9.4.1 一般
認証機関は，現地審査を実施するためのプロセスをもっていなければならない。このプロセスには，審査開始時の初回会議及び審査終了時の最終会議を含まなければならない。
審査の一部を電子的な手段によって行う場合，又は**審査対象の事業所が仮想（virtual）である場合**には，認証機関は，このような活動が，**適切な力量を備えた要員によって行われることを確実**にしなければならない。その審査中に得られる証拠は，審査員が，当該要求事項への適合性について，情報に基づいた決定ができるために，十分なものでなければならない。

注記 “現地”審査には，マネジメントシステムの審査に関連する情報を包含している電子的なサイトへの遠隔アクセスを含めることができる。審査の実施において，電子的な手段の使用を考慮することもできる。

- **審査の一部を電子的な手段によって行う場合**
  → **「主にコロナ感染予防のために行われるリモート審査（オンライン審査）は、認証機関に対する規格であるISO/IEC 17021-1：2015の9.4.1で示される「電子的な手段」で行われている」**
- **審査対象の事業所が仮想（virtual）である場合**
  → **最近のスタートアップ企業では、リアルのオフィスを持たず、全ての業務を仮想環境のオフィスで行っている事例（ISMSの審査も仮想環境に対して行う）**

4　認証範囲の基本的な考え方

4.1　認証範囲

MS規格を適用して認証を申請する範囲に対して、・・・適合性が証明された認証範囲

認証範囲は、**適用規格が取り扱う利害関係者に関連する、製品・サービスの一連の業務プロセス全体を含む**こと

4.2　認証範囲の確認

・・・申請範囲は組織の判断で設定されるため、機関は、**組織のプロセス、製品・サービス、関連サイト、事業部、事業所など**、適用規格の取り扱う側面に関連する直接/間接の影響を考慮し、**申請範囲の適切性を確認**する必要がある

直接的な管理下にある活動範囲のうち、**本来含めるべき活動を除外している場合、正当性を評価**し、正当と認められない場合は、認証を与えない

除外されている規格要求事項がある場合、その**要求事項の箇条が明確**になっていなければならない、**正当な理由**があり、**適切である**ことを確認

適用範囲が、**適用規格の意図に沿って適切に設定される**よう十分に配慮し、その**MSが全体として適合**しているか判断・・・

https://isms.jp/doc/JIP-IMAC121-11a.pdf

5. 認証文書への認証範囲の表記

・・・認証の利用者が**認証範囲に含まれる製品やプロセスを正しく理解できるよう、製品・サービス、プロセス、サイトなどに基づき正確かつ明確に表現**する必要がある

認証の利用者および市場に誤解を招くものではないことを確実にする・・・

認証の表記に次の事項を留意

a) 認証範囲に含まれる**製品・サービス、プロセス、サイトなどに関して、正確に把握できる**程度に詳細な表現をする
b) 認証範囲に含まれないサービス、・・・などへの言及、又はそれらが含まれると**誤解されるような表現はしない**
c) 組織の営業的要求に便宜を図るような表現はしない
d) **要求事項への適合に影響を与えるようなプロセスが外部委託されている場合、外部委託の程度を考慮**する

https://isms.jp/doc/JIP-IMAC121-11a.pdf

規格要求

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

（詳細は次ページ参照）

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

認証範囲の確認について

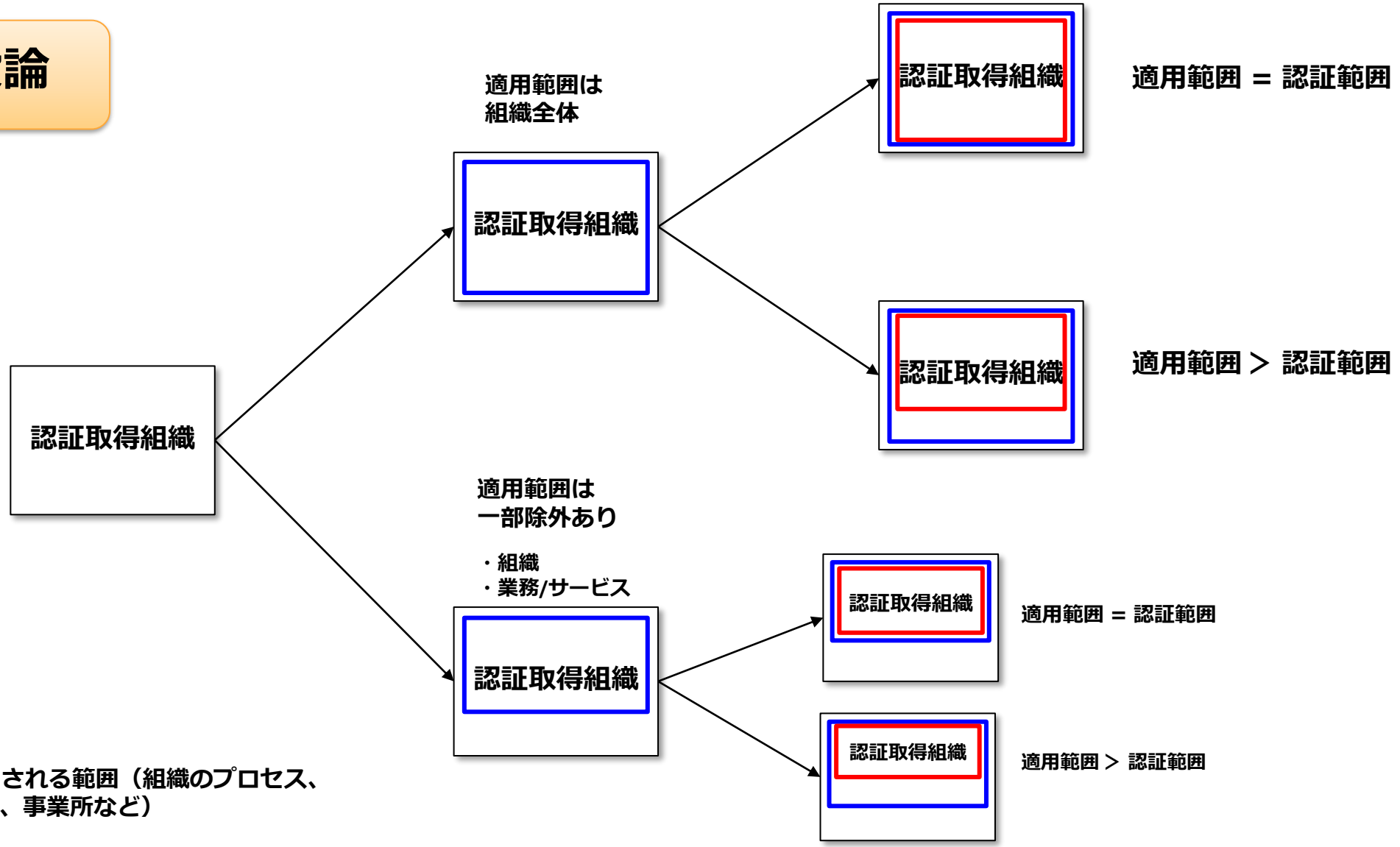
認証範囲の確認として下記の観点で行われる

組織のプロセス、製品・サービス、関連サイト、事業部、事業所など、適用規格の取り扱う側面に関連する直接/間接の影響を考慮し、**申請範囲の適切性を確認**する

- 直接的な管理下にある活動範囲のうち、**本来含めるべき活動を除外している場合、正当性を評価**し、正当と認められない場合は、認証を与えない
- **除外されている規格要求事項がある場合**、その**要求事項の箇条が明確**になっていること、**正当な理由**があり、**適切である**ことを確認
- 適用範囲が、**適用規格の意図に沿って適切に設定される**よう十分に配慮し、その**MSが全体として適合**しているか判断・・・

適用範囲と認証範囲について（イメージ図）

一般論



：適用範囲

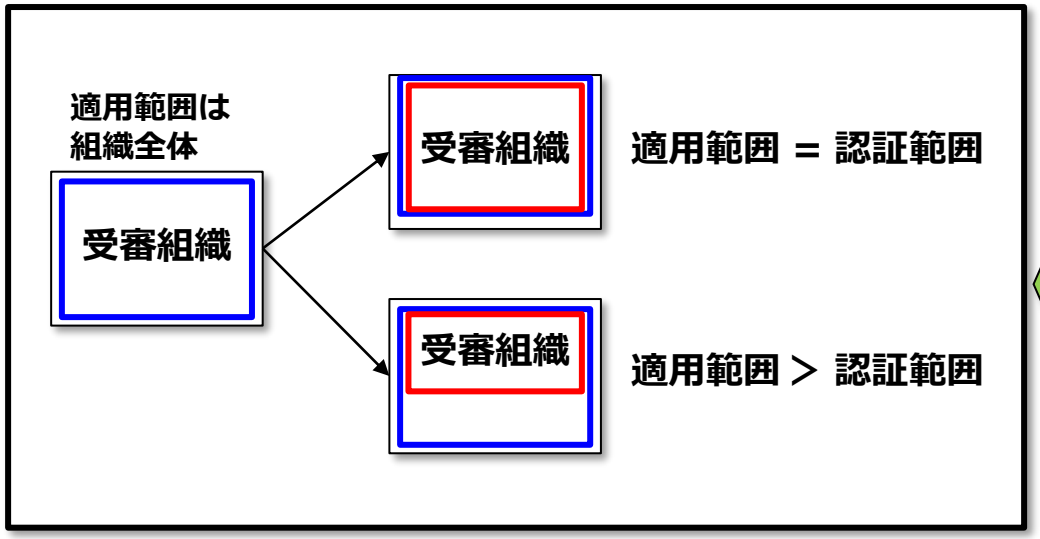
：認証範囲

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

組織としての適用範囲の決定から認証範囲の決定まで

組織としての適用範囲から認証範囲の正式決定までの大まかな流れを下記に示す
次ページ以降で組織として適用範囲の決定のプロセスについて示す

（受審組織）

適用範囲の決定 → 認証範囲の申請

「適用範囲定義書」

自組織としてどこまでの範囲にISMSを適用するのか判断する

（認証機関）

認証範囲の適切性の確認 → 認証範囲の決定

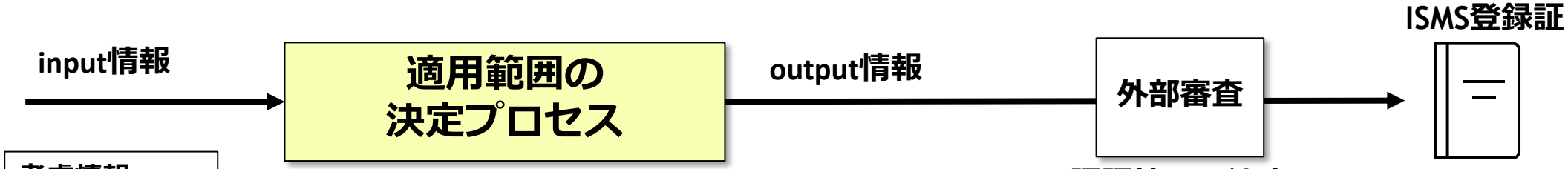
「ISMS登録証」

第三者から見た認証範囲について誤解を与えない

境界が明確になることでISMSの適用範囲の内外が可視化出来るのでセキュリティコントロールが明確になる

https://isms.jp/doc/JIP-IMAC121-11a.pdf

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

＋

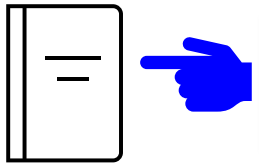
関連情報

- 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

参考　例：ISMS適用範囲定義書・・・適用範囲の文書化の事例

文書名	ＩＳＭＳ適用範囲定義書						
秘密区分	公開	管理番号	ISMS-01-20-1	管理組織	総合事務局	版数	1.3
JIS Q 27001:2014 適用　(ISO/IEC 27001:2013)　JIS Q 27017:2016 適用　(ISO/IEC27017:2015)　JIP-ISMS517-1.0							

当社のＩＳＭＳ適用範囲を以下に示します。

１．対象事業

（１）情報システム・ネットワークシステムに関するシステムインテグレーションサービス及び保守
（２）システム運用サービス及びヘルプデスク
（３）情報システムアウトソーシングサービス（印刷、封入、封緘）
（４）プロバイダとしての自治体向け総合行政クラウドサービス

２．適用組織

名 称　：株式会社北海道日立システムズ
公共社会事業部
企業サービス事業部
事業企画部
システム事業本部　システム第１部　第１グループ
第２グループ
システム第２部
プラットフォーム事業第１本部
ファシリティ事業推進部　ファシリティサービスグループ
プラットフォーム事業第２本部
営業統括本部
営業企画本部
公共・社会営業本部　営業第１部　営業第１グループ
営業第２部
企業営業本部　営業第１部　営業第１グループ
営業第２部
生産技術管理本部
品質保証本部

所在地　：北海道札幌市中央区大通西３丁目１１番地　北洋ビル
関連事業所
名称　：札幌オフィス
所在地　：北海道札幌市中央区北２条西４丁目１番地　札幌三井ＪＰビル　８Ｆ
対象業務：生産技術管理、品質保証業務
名称　：菊水分室
所在地　：北海道札幌市白石区菊水１条３丁目１番５号　メディア・ミックス札幌　３Ｆ
対象事業：上記「１．対象事業（１）」
適用要員　：役員、社員（派遣社員を含む）、常駐する委託会社社員
ただし、委託会社社員に対する指示は、委託会社の作業管理責任者を通じて行う。

３．物理的範囲

ＩＳＭＳを適用する物理的範囲はセキュリティレベルを「レベル３：事務室」、「レベル４：コンピュータ室、作業室等センタ関連区画、移送」、「レベル５：センタ関連区画内の高セキュリティエリア」に分類して定め、その物理的範囲及び境界は『ISMS-01-21-1 レイアウト図』に示します。（※1）

４．ネットワークの範囲

ＩＳＭＳを適用するネットワークの範囲は、ネットワークを利用するサービスの分類毎に定め、その範囲は『ISMS-01-20-1 ネットワーク図』に示します。（※1）

５．情報資産の範囲

ＩＳＭＳを適用する情報資産の範囲を以下に示します。なお、情報資産を扱う場所等が上記３～４項に該当しない場合であっても、本項の範囲に含まれる場合は適用範囲とします。

（１）適用組織が管理、又は使用する業務情報（業務用ファイル、各種申請書など）、社内文書（各種仕様書、手順書、契約書など）、社内記録（作業日報、チェックリストなど）、ソフトウェア（システムソフト、業務用ソフト等）印刷用紙、及びこれらの複製
（２）適用組織が管理、又は使用する運用機器（コンピュータ（サーバ、パソコン、端末）、ネットワーク機器（通信装置、通信回線等）、外部サービス（運用処理サービス、通信サービス等）
（３）上記（１）（２）の情報資産を保管、管理、取扱うための資産やこれらを扱う人材

※１：レイアウト図、及びネットワーク図は、当社の機密情報が含まれるため非公開としています。

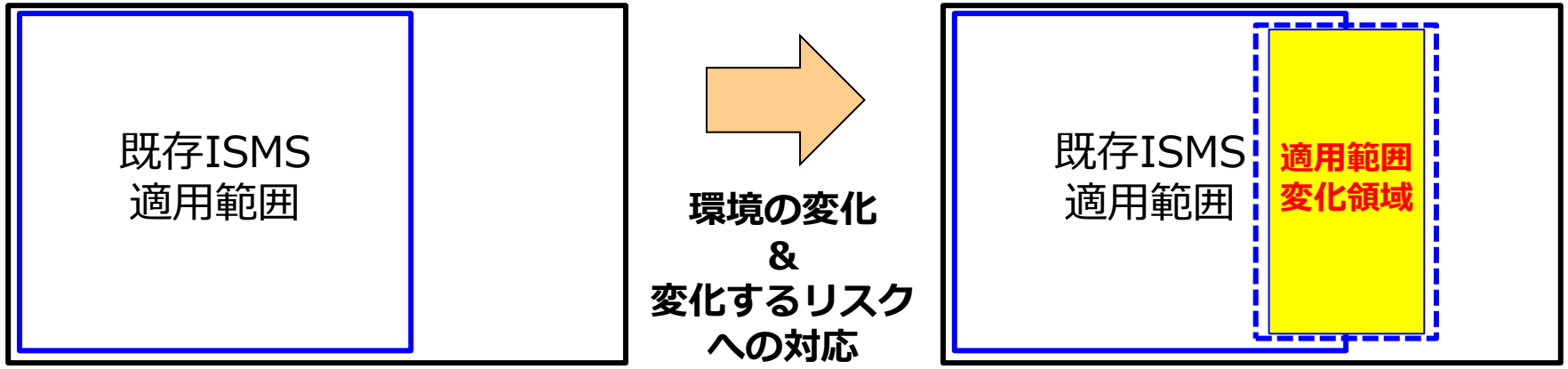
－１－

株式会社北海道日立システムズ

https://www.hokkaido-hitachi-systems.co.jp/image/hsl/ISMS-01-20-1.pdf

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

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）

最新の環境変化（クラウドへのマイグレ加速＆テレワークの定着）

主な最新の環境の変化としてクラウドシフトとテレワークの定着について下記に整理する

環境変化 その1	・オンプレからクラウドへのマイグレーションの加速 ・SaaS利用の拡大	・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
環境変化 その2	・出社前提からテレワークなどへのビジネススタイルの変化（仕事をする場所を選ばない） ・人による相互監視の前提条件が崩れている	・入退室管理が徹底した場所から割とオープンな場所での業務の実施 ・システムへアクセスするルートとして会社で管理しているセキュリティ対策済のNWからオープンなインターネット環境へのシフト ・物理よりも技術的な管理策にシフト

下記の観点で整理することで適用範囲の再定義を行う

・ISMSの適用範囲の仮設定

具体的な事例としてクラウドへのマイグレの加速と
テレワークの定着を題材として下記の流れで整理する

ア）

・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

外部/内部の課題や利害関係者のニーズなどの変化がもたらす影響の把握

イ）

・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

直接コントロール出来る範囲と間接コントロールの変化に着目

上記のア）とイ）を整理し、組織として
対応すべき全体像を可視化

・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

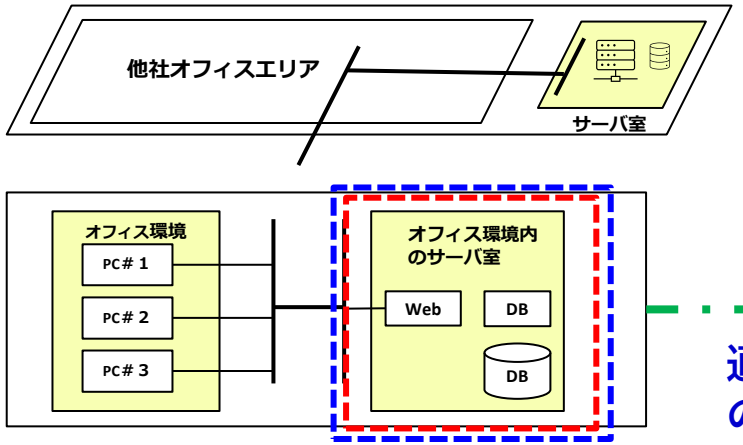
環境変化
その1

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

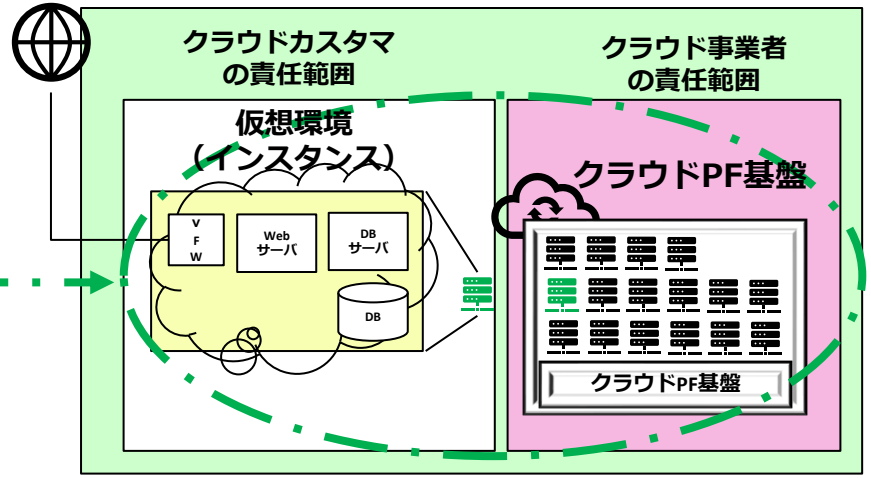
環境の変化 その１（オンプレからクラウドへのマイグレーション）

オンプレ中心のIT環境・・・情報資産は社内NW内に保管



適用範囲のオフィスサーバ群
のクラウド移行

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

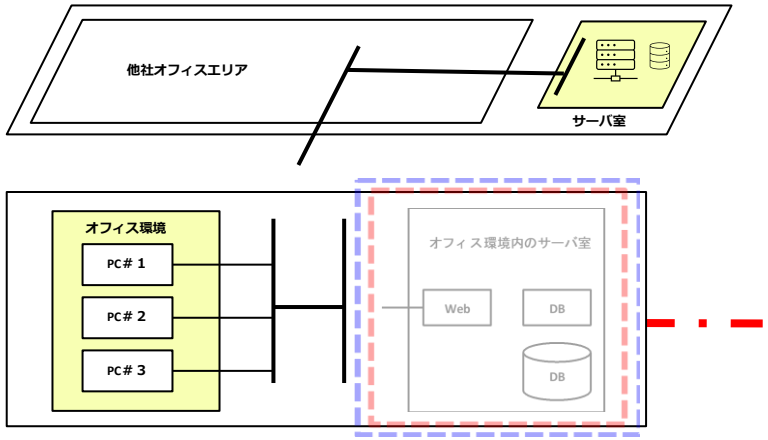
クラウド（仮想環境）

- 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

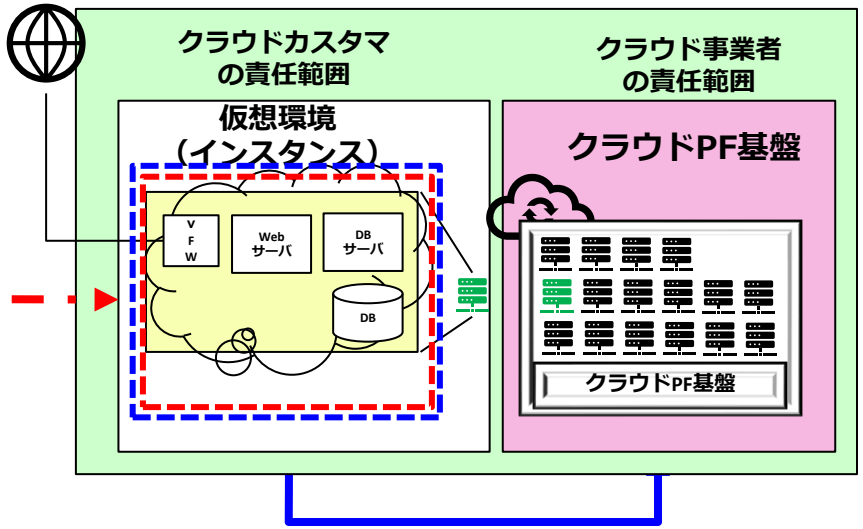
IaaS
事例

直接コントロール範囲（仮想環境）と間接コントロール範囲（クラウドPF基盤）について

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



クラウドの責任分界で整理（次ページ参照）

：適用範囲

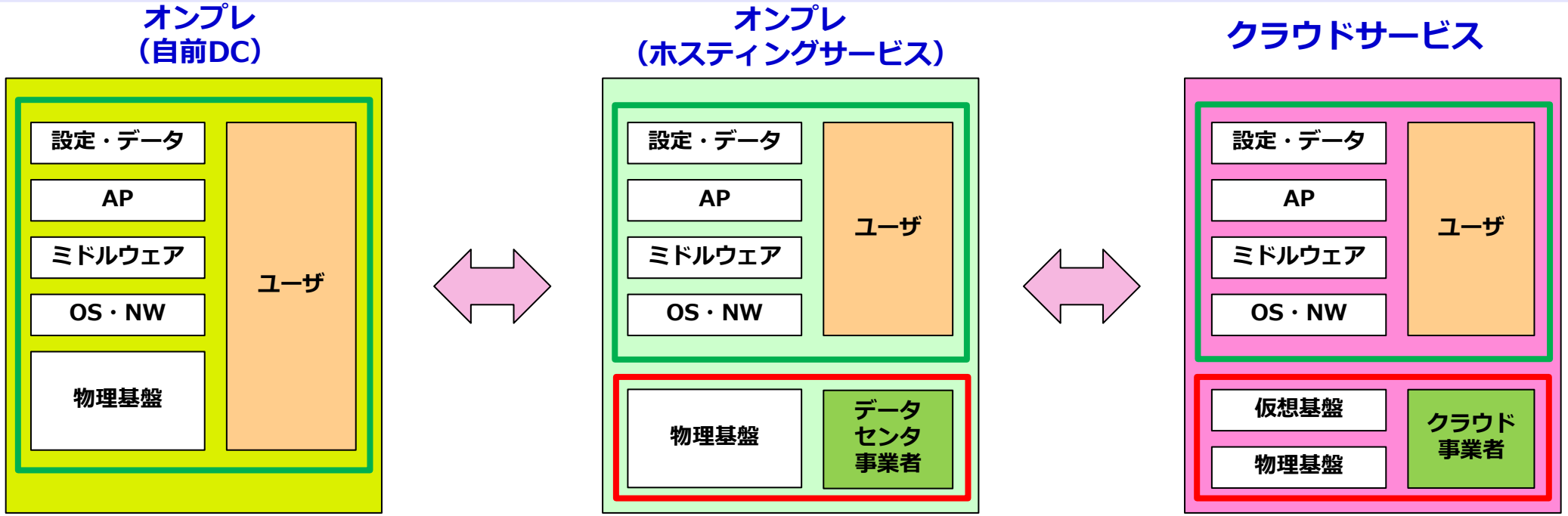
：認証範囲

マイグレで適用範囲として新たに定義

仮想環境を適用範囲、認証範囲として設定

A15 の供給者関係で整理

サービス契約毎のコントロール範囲の違いについて



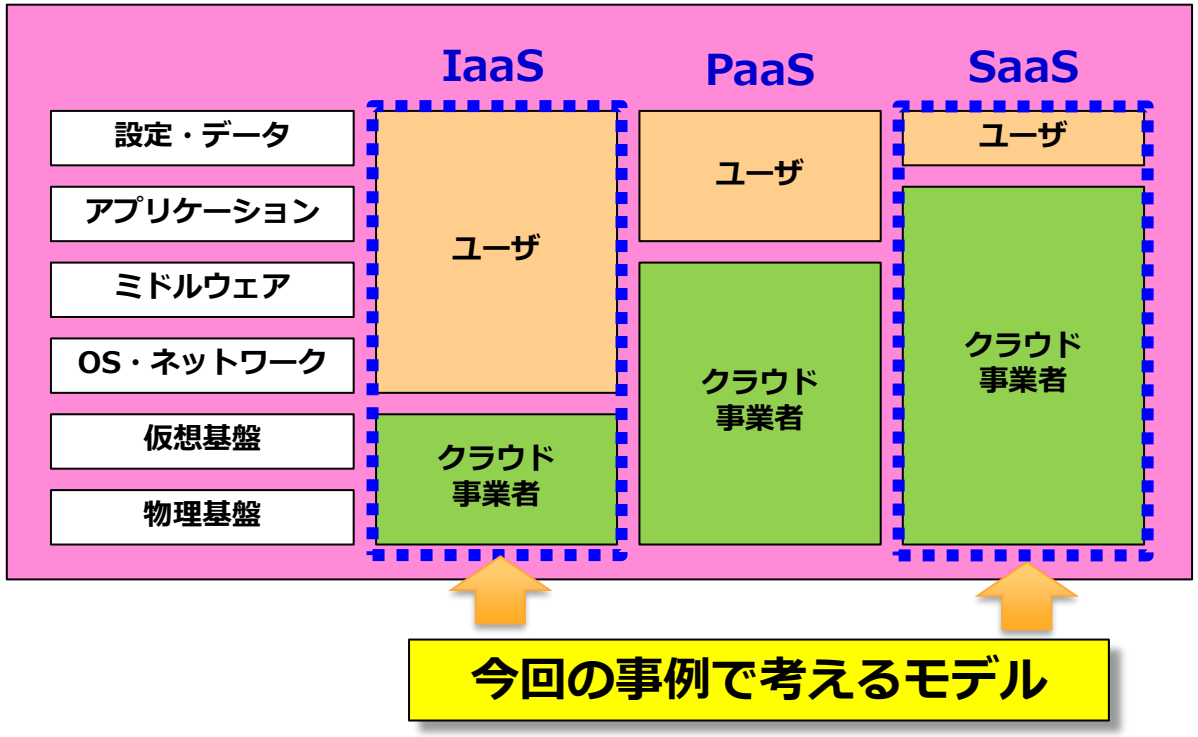
	自社のＤＣでシステムを運用（すべて自前）	業務委託（相対契約）	サービス利用（利用約款）
ユーザ		ホスティングサービス（システム基盤の提供）上のOSなどの上位層はユーザの責任範疇（直接コントロール）	仮想環境（インスタンス）についてはユーザの責任範疇（直接コントロール）
事業者		相対契約なのである程度契約条項に盛り込むことでコントロール可能	約款サービスに基づく契約のため、個別のコントロールは原則不可能

：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

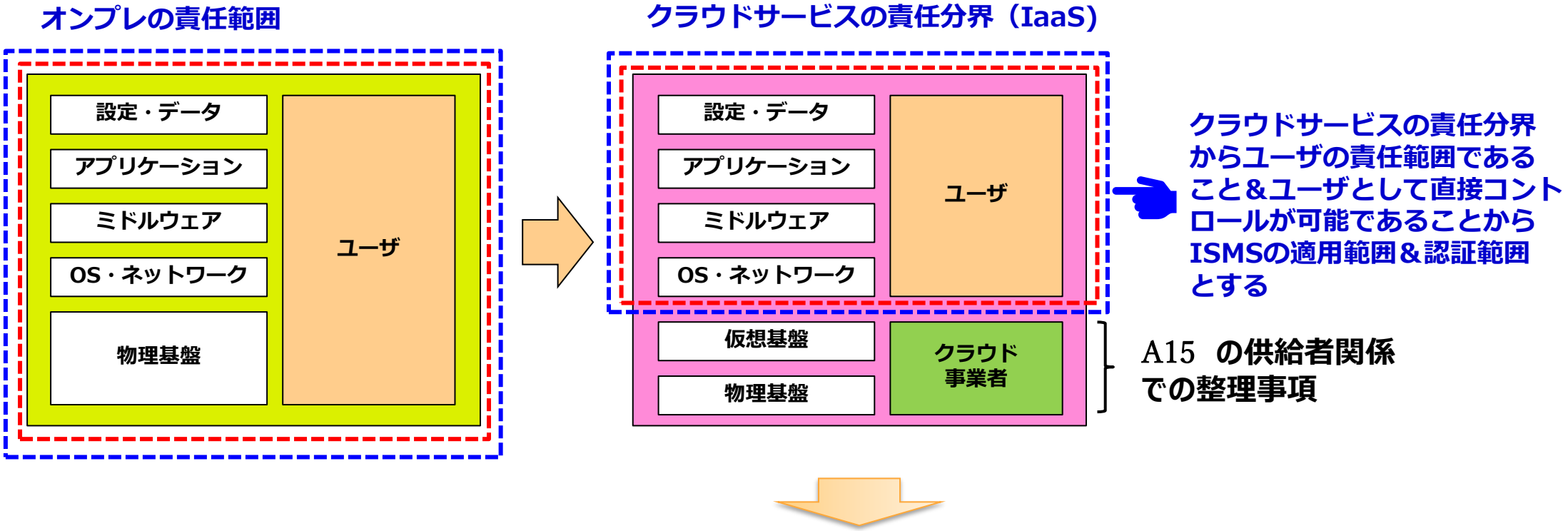


責任分界でユーザとクラウド事業者の境界線（直接コントロールが可能）が決まるが、最終的な結果責任は利用者に帰結するので、 A15 の供給者関係でも整理を行うことでトータル的なコントロール（ガバナンス）が可能となる

本パートではIaaSの事例で整理を行うが、後述のパートでSaaSの事例の整理も行う

IaaS
事例

環境の変化 その１（オンプレからクラウドへのマイグレーション）



：適用範囲

：認証範囲

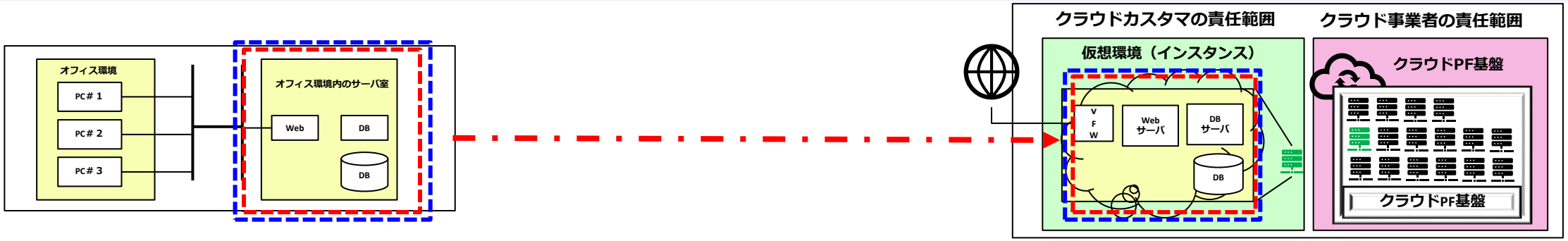
従来のオンプレからクラウドサービス（仮想環境）に移行

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

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

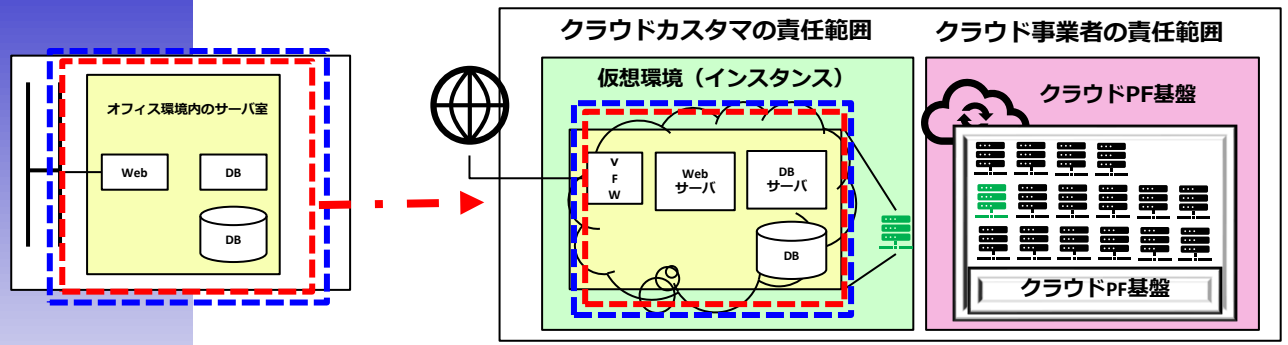
環境の変化（クラウドシフト）に関する考慮事項（箇条4.3）

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
移行だけでなく右記に示す箇条4.3の要求
事項を考慮した検討プロセスが必要となる

＋α

箇条4.3の要求事項の考慮ポイント

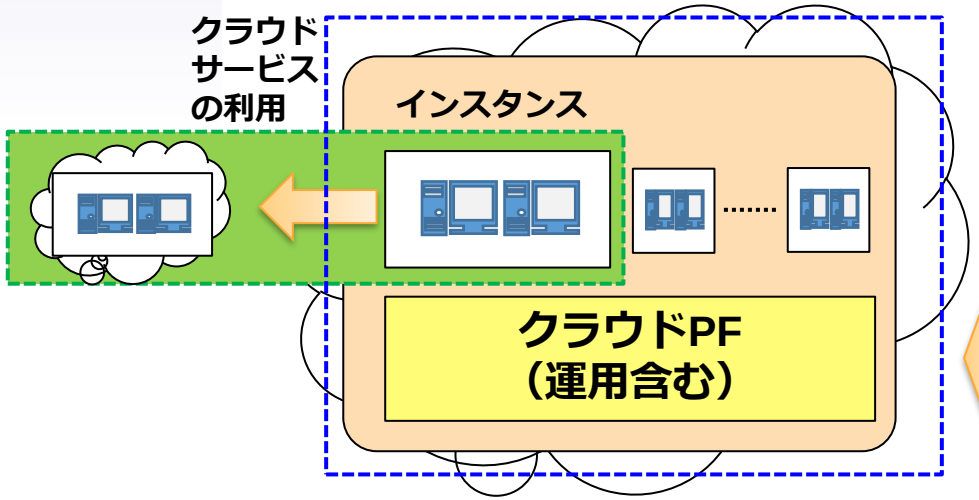
○外部の課題
　法令やガイドラインへの対応
　（約款の確認、国内リージョン指定など）
○内部の課題
　クラウド利用のガイドラインの制定＆教育
　従業員研修
○利害関係者のニーズ及び期待の理解
　インターネット上でシステムや機密情報が
　適切に管理運用されていること
○組織が実施する活動と他の組織が実施する活動
　との間のインフェース及び依存関係
　クラウド責任分解モデルやA15供給者との関係で整理
　コントロール内、コントロール外での管理策の考えに
　基づき整理を行い、必要に応じて追加の管理策の検討
　→ISMAPを利用した要件の確認（次ページ参照）

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）

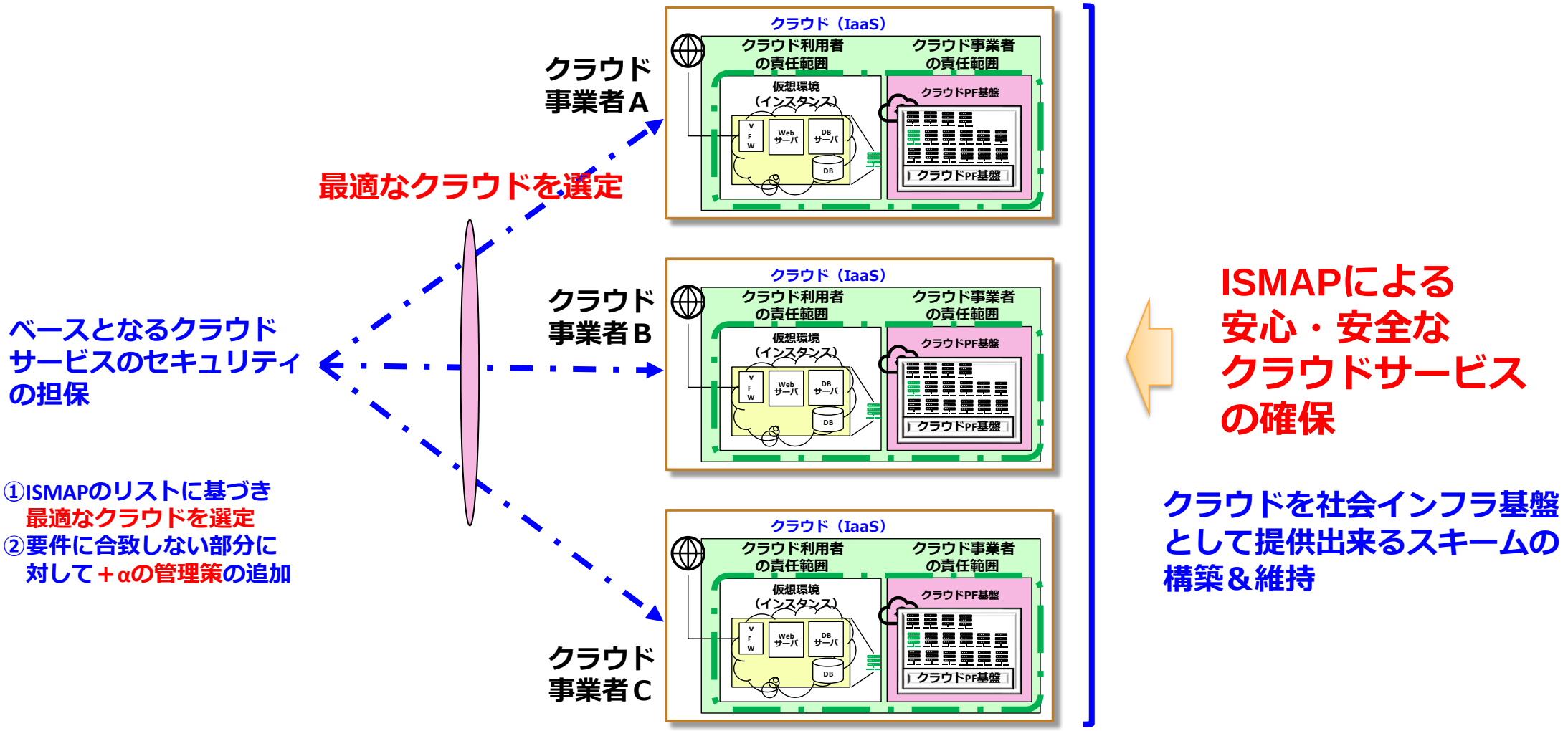


ISMAPによる安心・安全なクラウドサービスの確保

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**

参考：ISMAPを利用した要件の確認



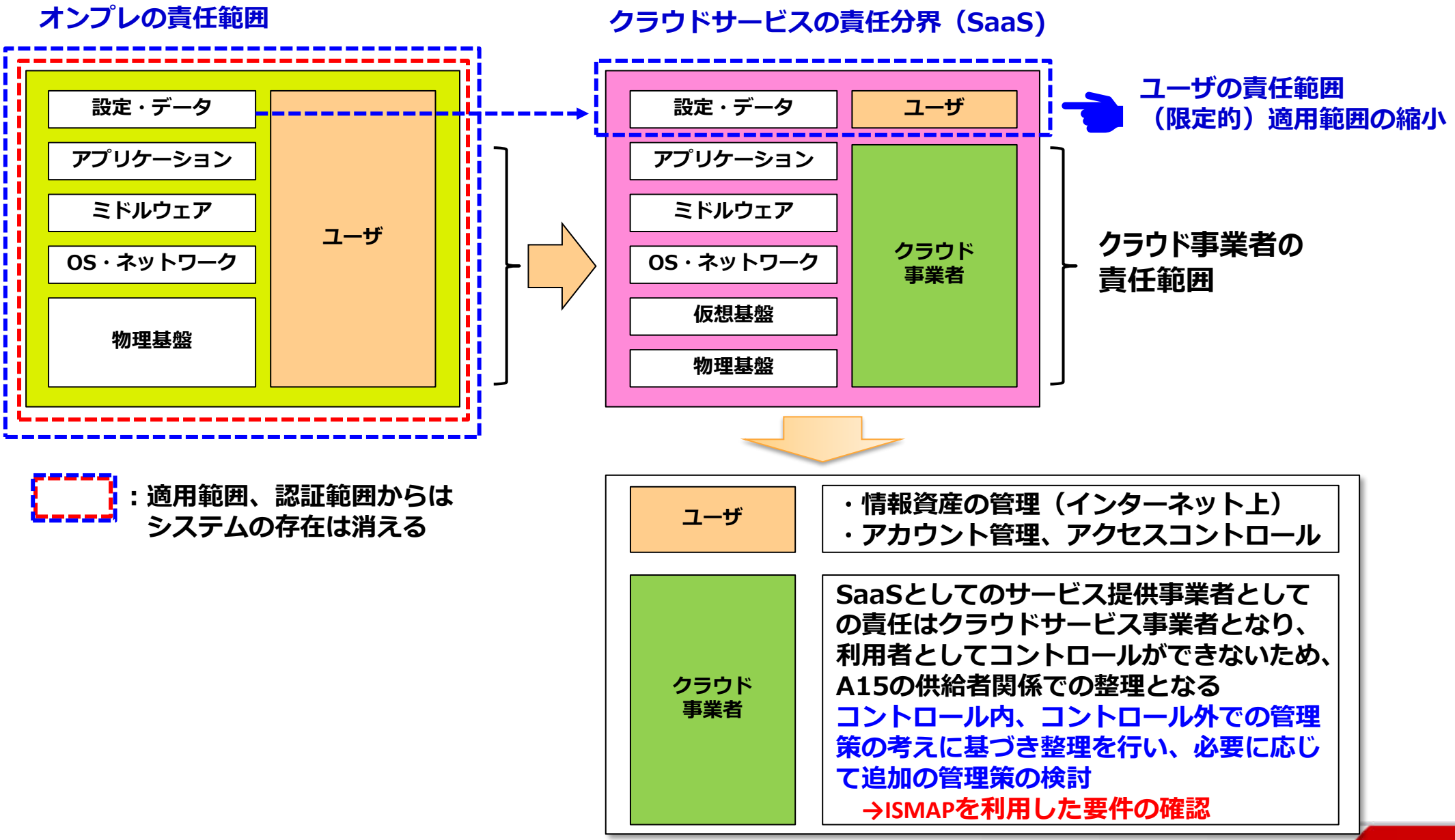
環境変化
その1

補足

SaaSの事例

SaaS
事例

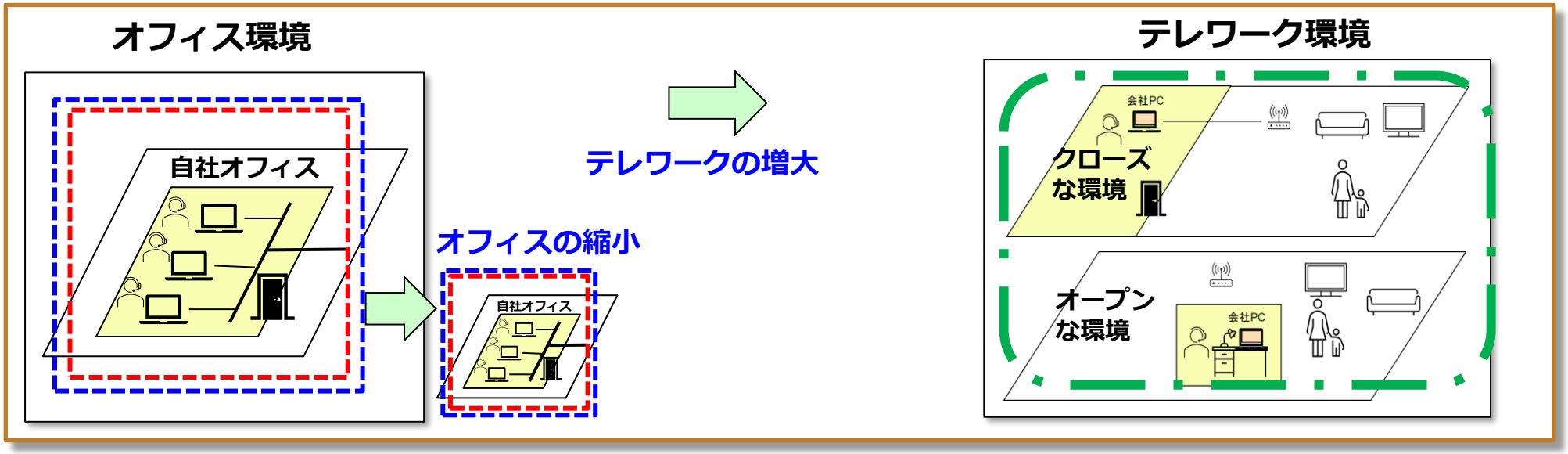
環境の変化 その１（オンプレからクラウドへのマイグレーション）



環境変化
その2

テレワークの定着

テレワークへの移行時のコントロールの変化について



直接コントロール出来る領域

間接的にコントロールする領域

直接コントロール出来る領域

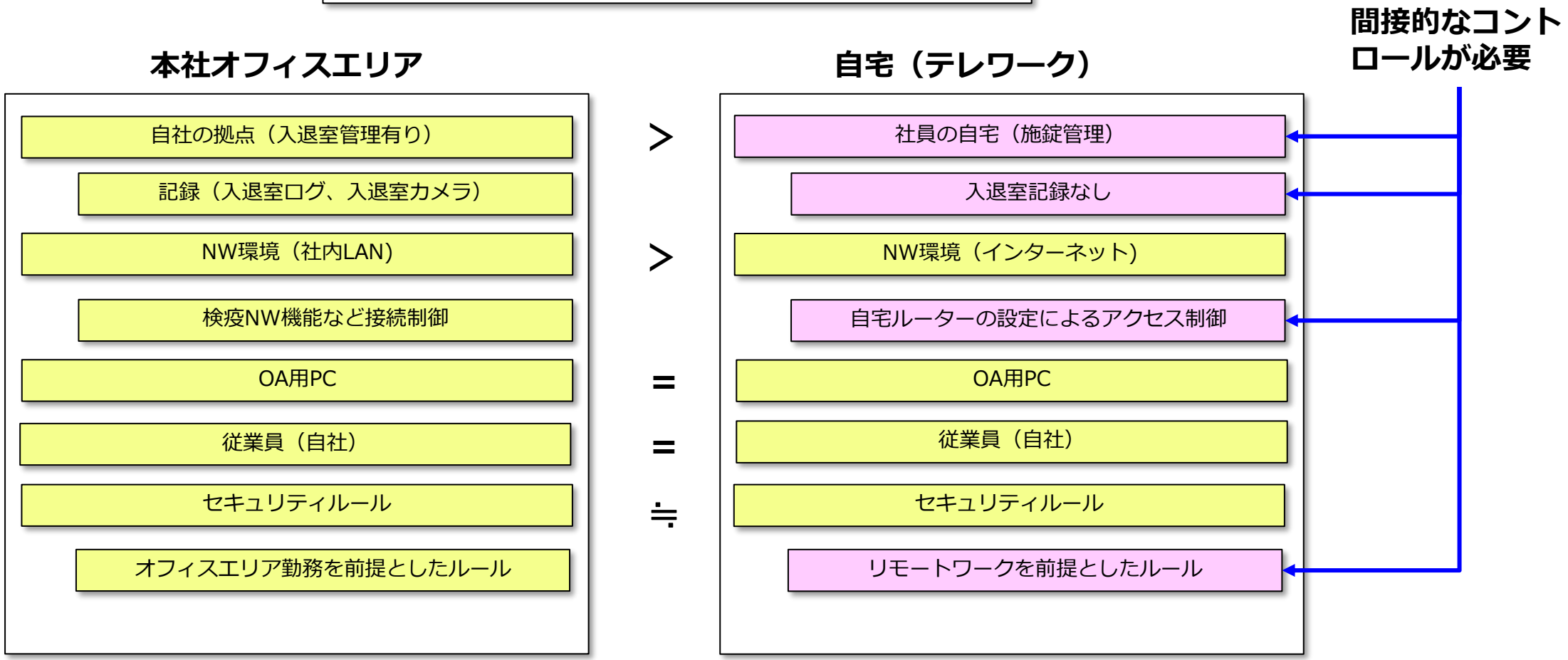
間接的にコントロールする領域

：適用範囲

：認証範囲

オフィスエリアとテレワーク環境の相異について

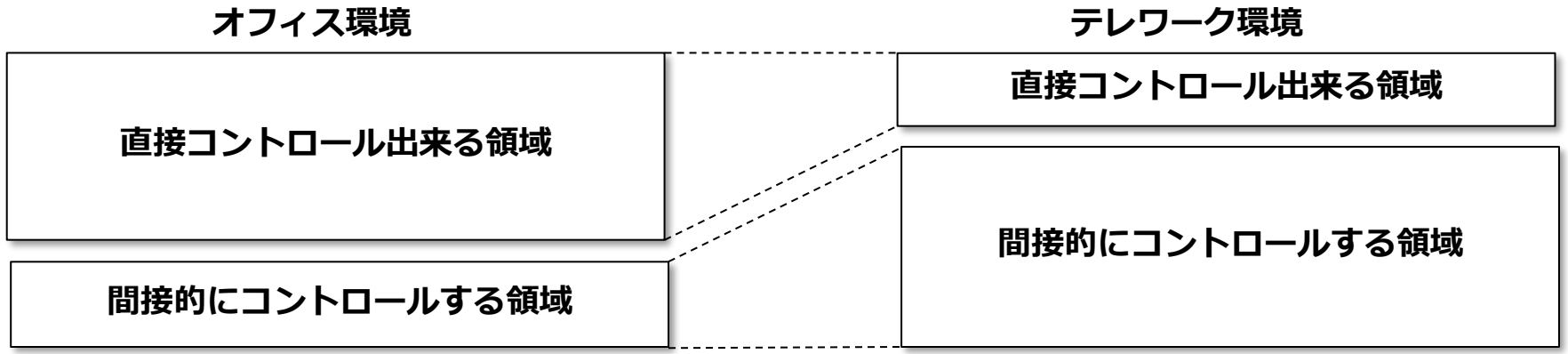
組織と従業員とで責任分界で管理を分ける



：直接コントロール出来る領域

：間接コントロールが必要な領域

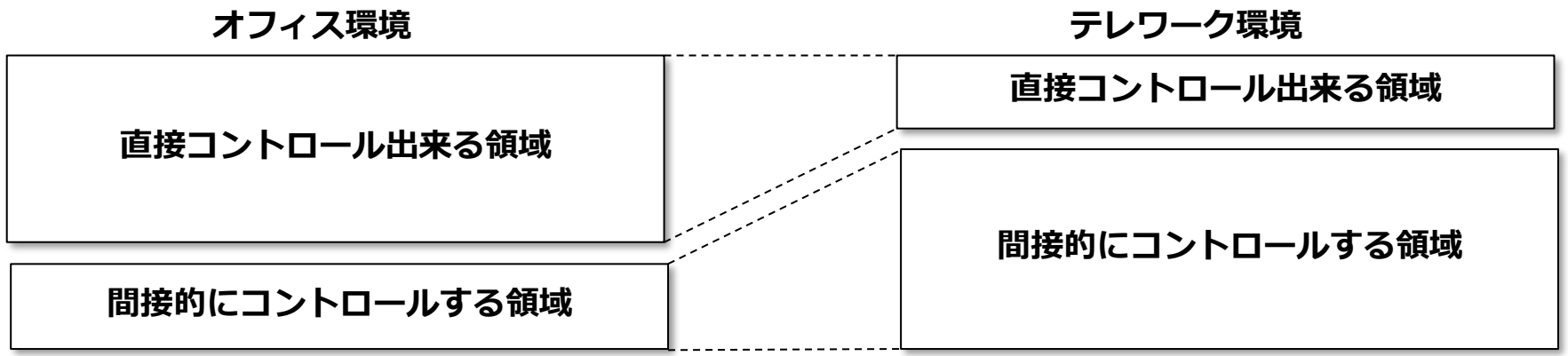
テレワークへの移行時のコントロールの変化について



分類	コントロールの要素	備考
直接コントロール出来る領域	・NW環境（インターネットからの社内システムへの入り口） ・OA用PC（会社貸与） ・従業員（自社） ・セキュリティルール（従来のもの）	入退出管理システムや情報システムなどで強制的にアクセス管理する
間接的にコントロールする領域	・社員の自宅の施錠管理 ・自宅のネットワーク環境 ・リモートワークにおけるルール （間接コントロールするためのガイドラインや誓約書等によるガバナンスの確保）	ルールや誓約書などで間接的に管理

参考事例：テレワークへの移行時のコントロールの変化について

事例（その1）　会議内容が見られる、聞かれるリスク



直接コントロール出来る領域

→ICカードを使用した入退室管理により、オフィスエリアへの第3者の立ち入りを制限
→会議室で会議することで関係者以外に聞かれない

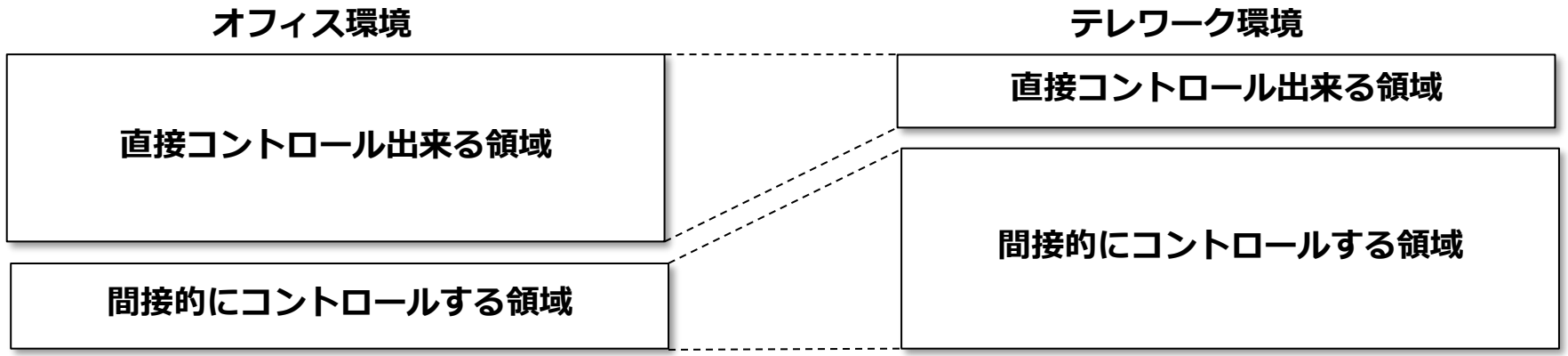
間接的にコントロール出来る領域

→入退室管理は無いが、出来るだけ自分だけのスペースを確保する（努力範囲）
→画面に覗き見防止フィルターを装着する
→会議の音が漏れない様に、イヤフォン、ヘッドフォン等を使い、リモート会議を実施する

・ルール策定＆周知
・覗き見防止フィルターなどの物品配布

参考事例：テレワークへの移行時のコントロールの変化について

事例（その2）　安全でないNW回線を利用することによる盗聴リスクなど



直接コントロール出来る領域

→セキュリティ対策（検疫NWなどの導入）によりシステムで許可したPC以外の排除する
→アクセスルートも物理エリアにて守られた社内LAN経由に限定

間接的にコントロール出来る領域

→システムへアクセスするルートとしてオープンなインターネット環境（特にwifi）への第3者からのアクセス排除（暗号化モード：WPA2 Personal AES、MACアドレスによる制限、隔離機能など）
→不正なPCからアクセスポイントに侵入されていないかチェック

- 安全なNW設定についてのルール策定＆周知
- アクセスポイント設定についての勉強会の開催など
- 安全なNW設定のガイドラインの策定＆提示

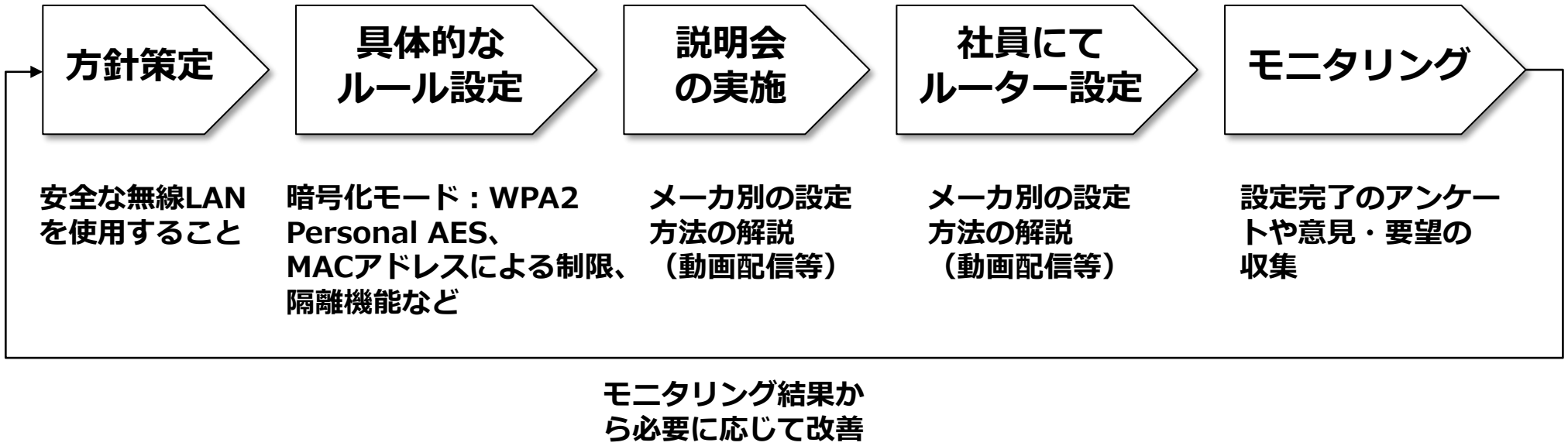
安全な無線LANの管理　https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/08.html

https://www.soumu.go.jp/main_content/000803351.pdf

事例：テレワーク時のwifiルーターの間接的コントロールについて

実際の事例としては従業員任せとなっていることが多いが、ITリテラシーのばらつきを考慮すると下記のような対応が望ましい

- 順守事項の明確化（ルールの制定＆具体的な手順書の提示）
- 従業員への教育/訓練の実施によるスキル習得＆意識づけ
- 必要に応じて誓約書の取得



環境の変化（テレワークの定着）に関する考慮事項（箇条4.3）

規格要求事項	環境の変化に伴う新たな要求事項	備考
外部及び内部の課題（組織及びその状況の理解）	【外部の課題】 ・ステークホルダーとの関係 お客さま、パートナー企業（派遣社員含む）との連携（ワークスタイルの乖離の有無） ・多様で柔軟な働き方へのシフトの時代の要求（企業の先進性が求められる） →育児、介護、住環境の選択の自由など ・サイバー攻撃のリスク増（インターネット経由での社内インフラへのアクセス） ・自由に働き場所が選べる ・テレワーク環境の確保が個人毎に異なる（通信環境や住環境などのインフラ） ・業種毎に適用に差異が発生 【内部の課題】 ・コミュニケーションが取りにくい（ノンバーバルによるコミュニケーションが減る） 顔出しなどのプライバシー問題との兼ね合い →顔出し前提や会議での発言で誰かが判明するので、コロナ禍でのオフィスにおける マスク状態で誰が出社しているのかわからない状態より良いか？ ・ITリテラシーが求められる ・内部不正における相互牽制が働きにくい ・テレワーク適用コスト（企業側のインフラ）の負担 -ディジタル化・ペーパレス化、Web会議、セキュリティ対策、シンクラPCなど	

環境の変化（テレワークの定着）に関する考慮事項（箇条4.3）

規格要求事項	環境の変化に伴う新たな要求事項	備考
要求事項（利害関係者のニーズ及び期待の理解）	・お客様、パートナー企業との関係（テレワーク導入企業と未導入企業）→ハイブリッド お客さま、パートナー企業（派遣社員含む）との連携（ワークスタイルの乖離の有無） ・機密情報の保持（お客さまからの預託情報などのアクセス管理や保護）	
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	自社、お客さま、パートナー企業とのコミュニケーションインターフェースの整理	

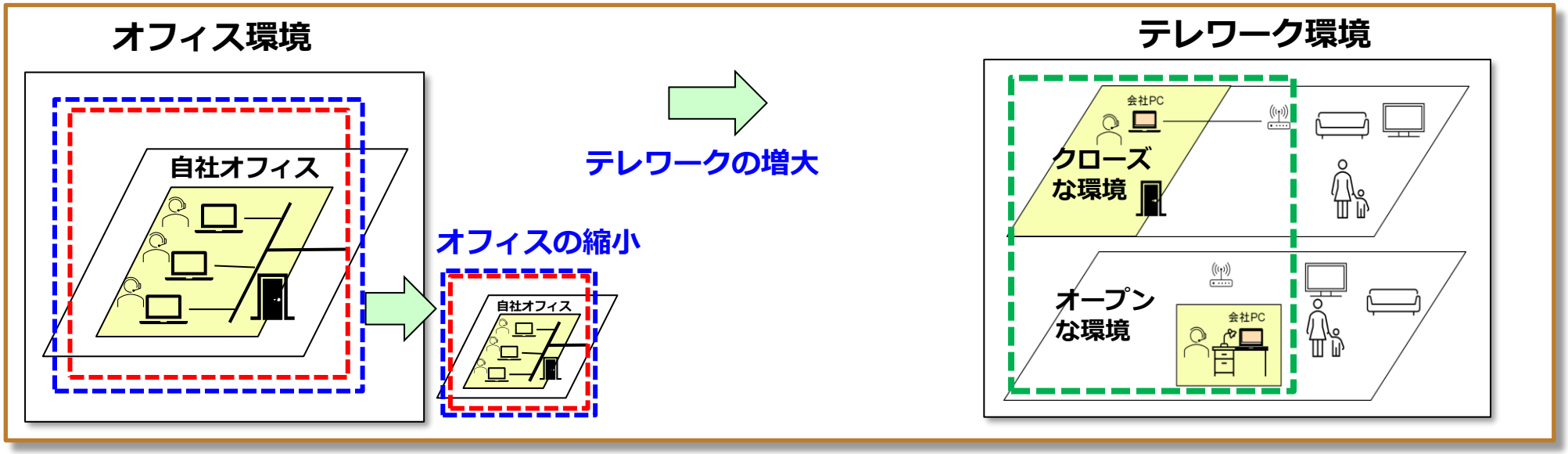
環境の変化（テレワークの定着）に関する考慮事項（箇条4.3）

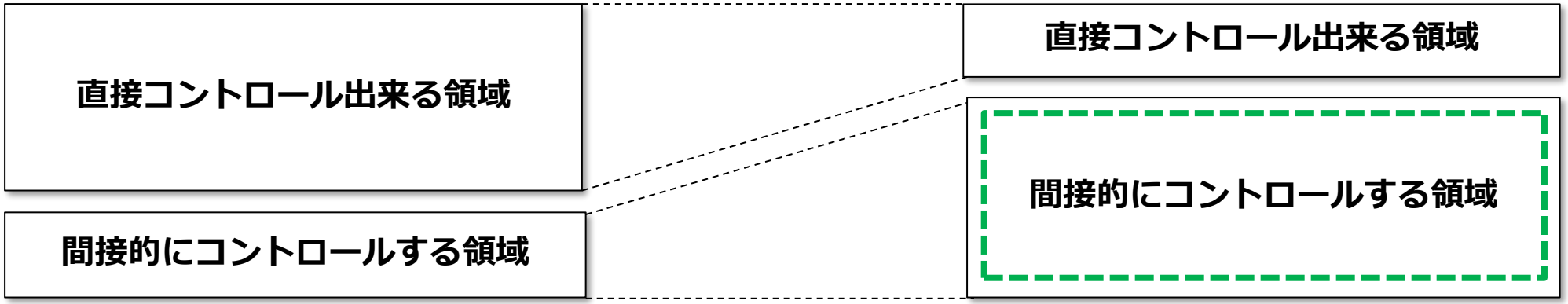
項目	要求される対応項目	対応方針	備考
外部の課題	・ステークホルダーとの関係 お客さま、パートナー企業（派遣社員含む）との連携（ワークスタイルの乖離の有無）	組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係の整理と並行して適切なコミュニケーション手段を選択する	
	・サイバー攻撃のリスク増（インターネット経由での社内インフラへのアクセス）	テレワーク運用コストとしてサイバー攻撃対策としてIT環境の整備（セキュリティ対策含む）を実施	
	・テレワーク環境の確保が個人毎に異なる（通信環境や住環境などのインフラ）	必要に応じてテレワーク環境の支援（サテライトオフィス、モバイルルーターの貸与など）でテレワーク難民を作らない	
内部の課題	・ITリテラシーが求められる	テレワークだとトラブル時に画面を見ながらのアドバイスなどを受けられないので、ITリテラシーの向上施策や社内ヘルプを充実させる	
	・内部不正における相互牽制が働きにくい	社内環境、テレワーク環境共に相互牽制が働きにくくなることから、ログのモニタリングなどによる強化を図ると共に意識づけ強化の研修の実施	
	・テレワーク適用コスト（企業側のインフラ）の負担 -ディジタル化・ペーパレス化、Web会議、セキュリティ対策、シンクラPCなど	IT化に必要な予算を計画的に計上する（セキュリティ対策はリスクに応じて優先度づけ）	

環境の変化（テレワークの定着）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	・お客様、パートナー企業との関係（テレワーク導入企業と未導入企業）→ハイブリッド お客さま、パートナー企業（派遣社員含む）との連携（ワークスタイルの乖離の有無）	テレワーク導入によるステークホルダーとのコミュニケーションギャップの防止 →自社の要求事項だけでなく、相手先との調整を実施しながら、新たなワークスタイルを模索する	
	・機密情報の保持（お客さまからの預託情報などのアクセス管理や保護）	リスクマネジメントの徹底による機密情報の保護 →前述の外部、内部の課題への対応を確実に実施することで、リスクマネジメントを徹底する	
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	自社、お客さま、パートナー企業とのコミュニケーションギャップの防止	自社、お客さま、パートナー企業とのコミュニケーションインターフェースの整理 →齟齬が発生しないように適切にマネジメントする 例）社員がテレワーク、派遣社員だけが出社というような歪な状況だとコミュニケーション齟齬が発生する可能性がある	

テレワークへの移行時のコントロールの変化について



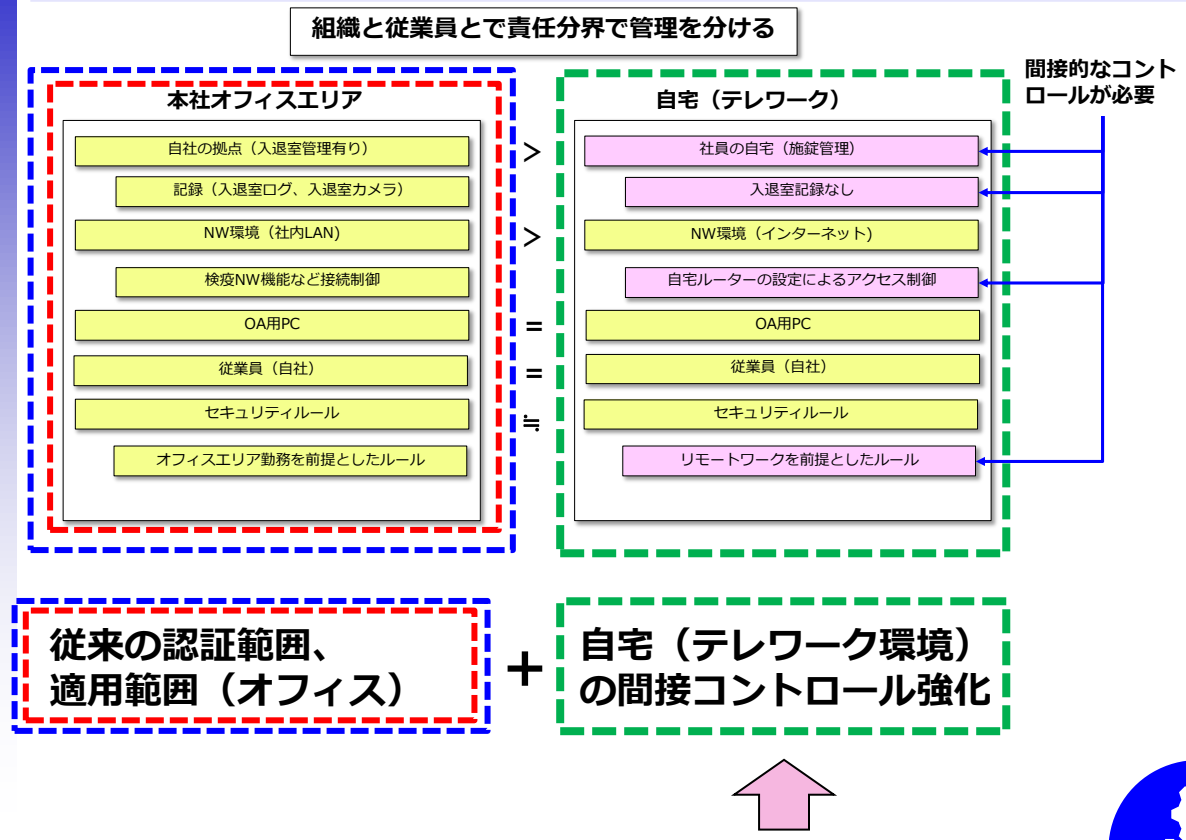


：適用範囲

：認証範囲

ルールや誓約書等で社員に間接コントロールする
ことでセキュリティガバナンスを維持・向上

適用範囲見直しにおける考慮ポイント・・・テレワークの定着



ルールや誓約書等で社員に間接コントロールすることでセキュリティガバナンスを維持・向上

直接コントロール

間接コントロール

：適用範囲

：認証範囲

＋α

箇条4.3の要求事項の考慮ポイント

○外部の課題
- 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の整備
- サイバー攻撃対策としてIT環境の整備
- テレワーク環境の支援

○内部の課題
- ITリテラシーの向上施策や社内ヘルプを充実
- ログ監視などによるモニタリング強化
- 意識づけ強化の研修の実施
- IT化に必要な予算を計画的に計上

○利害関係者のニーズ及び期待の理解
- テレワーク導入によるステークホルダーとのコミュニケーションギャップの防止
- リスクマネジメントの徹底による機密情報の保護

○組織が実施する活動と他の組織が実施する活動
- 自社、お客さま、パートナー企業とのコミュニケーションインターフェースの整理

まとめ

まとめ

適用範囲の決定プロセス

・ISMSの適用範囲の仮設定

ア）
・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

外部/内部の課題や利害関係者のニーズなどの変化がもたらす影響の把握

イ）
・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

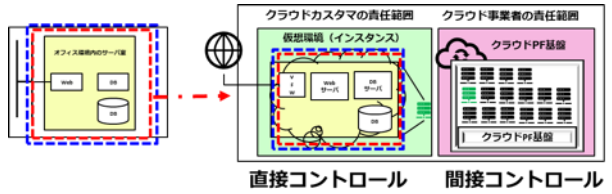
直接コントロール出来る範囲と間接コントロールの変化に着目

上記のア）とイ）を整理し、組織として対応すべき全体像を可視化

・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適用範囲が正式決定

事例1：クラウドへのマイグレ加速に伴う適用範囲の変化とリスク対応



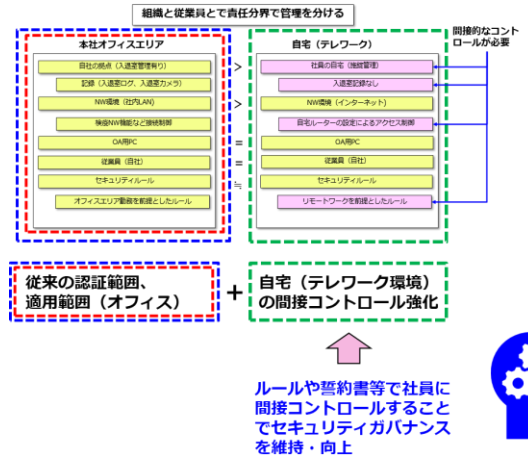
単純にリアルマシンから仮想マシンへの移行だけでなく右記に示す箇条4.3の要求事項を考慮した検討プロセスが必要となる

＋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）

事例2：テレワークの定着に伴う適用範囲の変化とリスク対応



＋α

箇条4.3の要求事項の考慮ポイント

○外部の課題
　・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の整理
　・サイバー攻撃対策としてIT環境の整備
　・テレワーク環境の支援
○内部の課題
　・ITリテラシーの向上施策や社内ヘルプを充実
　・ログ監視などによるモニタリング強化
　・意識づけ強化の研修の実施
　・IT化に必要な予算を計画的に計上
○利害関係者のニーズ及び期待の理解
　・テレワーク導入によるステークホルダーとのコミュニケーションギャップの防止
　・リスクマネジメントの徹底による機密情報の保護
○組織が実施する活動と他の組織が実施する活動
　・自社、お客さま、パートナー企業とのコミュニケーションインターフェースの整理

最新の環境の変化（クラウドへのマイグレ加速やテレワークの定着）を事例として適用範囲の変化やリスク対応を見てきました
環境の変化が起こった場合には個々の管理策の確認だけでなく規格に立ち返って確認することでリスクの変化を見逃さないようなプロセス作りにつなげることが重要と判断します

■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： 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

テーマ2： 続・効率的リスクアセスメント

現在、Web会議（zoom）で討議しています！
毎月最終木曜日18:00～21:00

ご清聴ありがとうございました

JNSA 標準化部会
日本ISMSユーザグループ
インプリメンテーション研究会

また、来年本セミナーでお会いしましょう

JNSA 標準化部会
日本ISMSユーザグループ
インプリメンテーション研究会