2017/12/13

# クラウドサービスセキュリティ環境及びサイバーセキュリティ環境における複数組織間のISMSのあり方への考察


工学院大学情報学部

ISO/IEC JTC1/SC27/WG1主査

やまさき　さとる

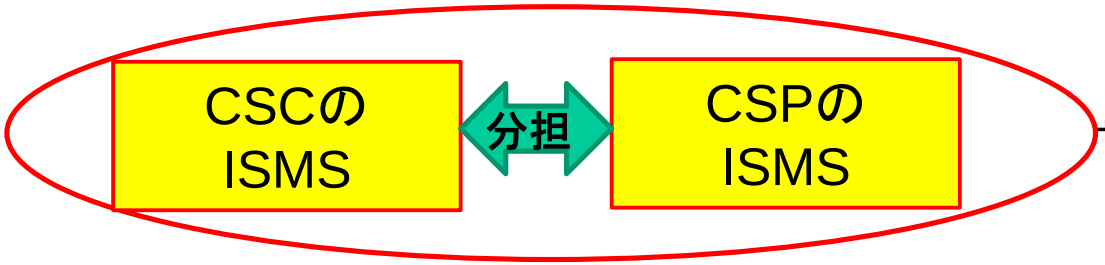
山﨑　哲

# 複数組織間におけるISMS適用の考え方

1.


情報セキュリティ
マネジメントシス
（ISMS）

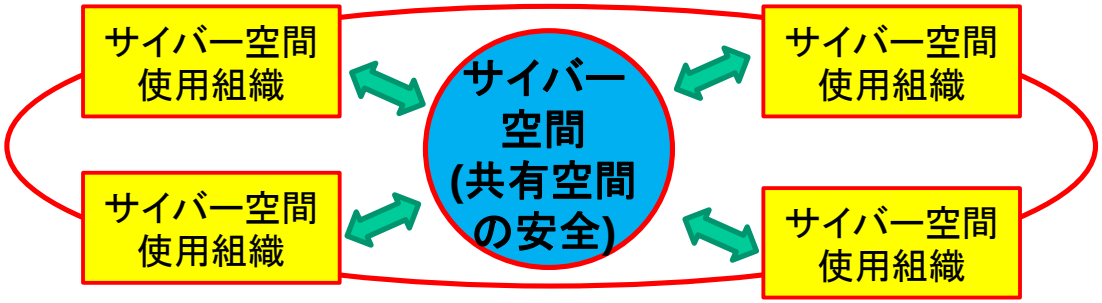
2.




クラウド
サービス
環境

クラウド
サービス
セキュリティ
環境

3.




サイバー
空間

サイバー
セキュリティ
環境

# ご説明内容

1. **単一組織の情報セキュリティマネジメントシステム（ISMS）**
   (1) 情報セキュリティマネジメントシステム（ISMS）の基本的要素
   (2) Integrated Management Systems Standards(IMSS)の適用に関する考え方
2. **クラウドサービスセキュリティ環境におけるISMS適用の考え方**
   (1) クラウドサービスセキュリティ環境におけるISMSの構造
   (2) 局面毎のISMSの役割と機能
   - 局面１：クラウドサービス合意
   - 局面２：情報セキュリティ方針設定
   - 局面３：情報セキュリティ目的/目標の設定
   - 局面４：リスクマネジメントの実施
   - 局面５：管理策の導入と運用
   - 局面６：監視・測定・分析・評価の実施
3. **サイバーセキュリティ環境におけるMS適用の考え方**
   (1) サイバーセキュリティ環境におけるMSの構造
   (2) 局面毎のMSの役割と機能
   - 局面１：サイバー空間使用ルールの合意
   - 局面２：サイバーセキュリティ方針設定
   - 局面３：サイバーセキュリティ目的/目標の設定
   - 局面４：リスクマネジメントの実施

# (1)情報セキュリティマネジメントシステム（ISMS）の基本的要素 – 情報セキュリティ分野におけるマネジメントシステム -

- **マネジメントシステムとは何か**

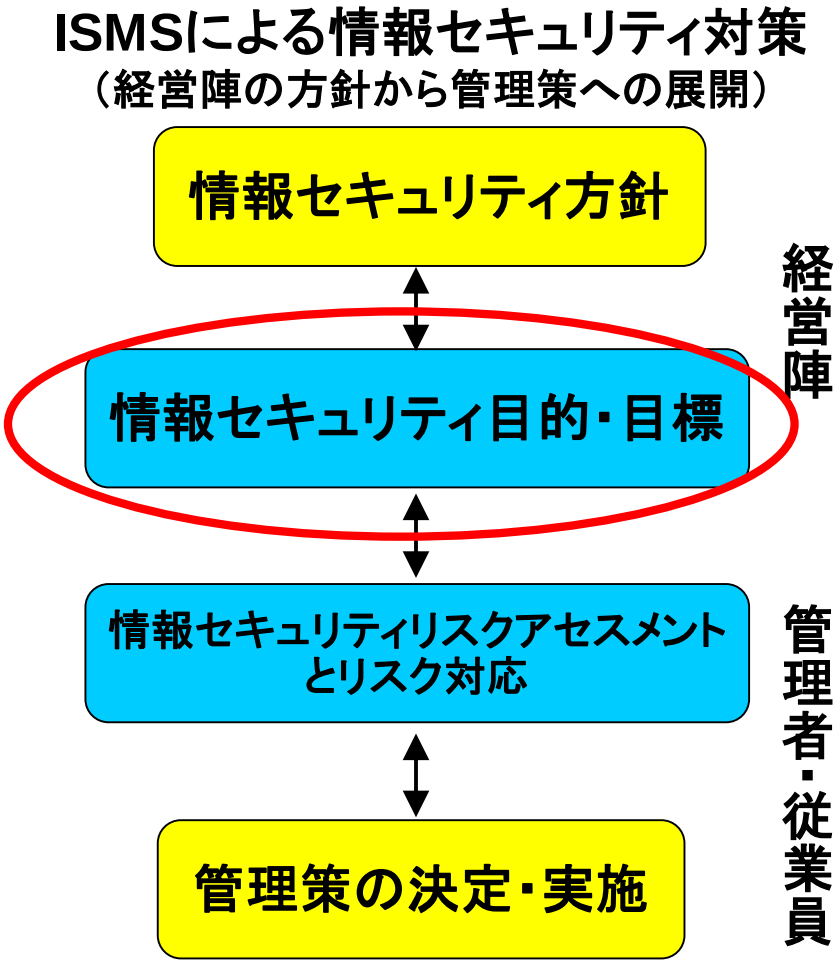
  方針、目的及びその目的を達成するためのプロセスを確立するための、相互に関連する又は相互に作用する、組織の一連の要素

- **ISMSとは何か**

  情報セキュリティ分野におけるマネジメントシステムが、情報セキュリティマネジメントシステム(ISMS)である。

  従って、ISMSとは、情報セキュリティの確立、実施、維持、継続的な改善によって、その**組織の目的**を達成するプロセスを確立するための、相互に関連又は相互に作用する一連の要素（組織の構造、役割及び責任、計画、運用など）のことである。

# (1)情報セキュリティマネジメントシステム（ISMS）の基本的要素 – 情報セキュリティ目的・目標 -

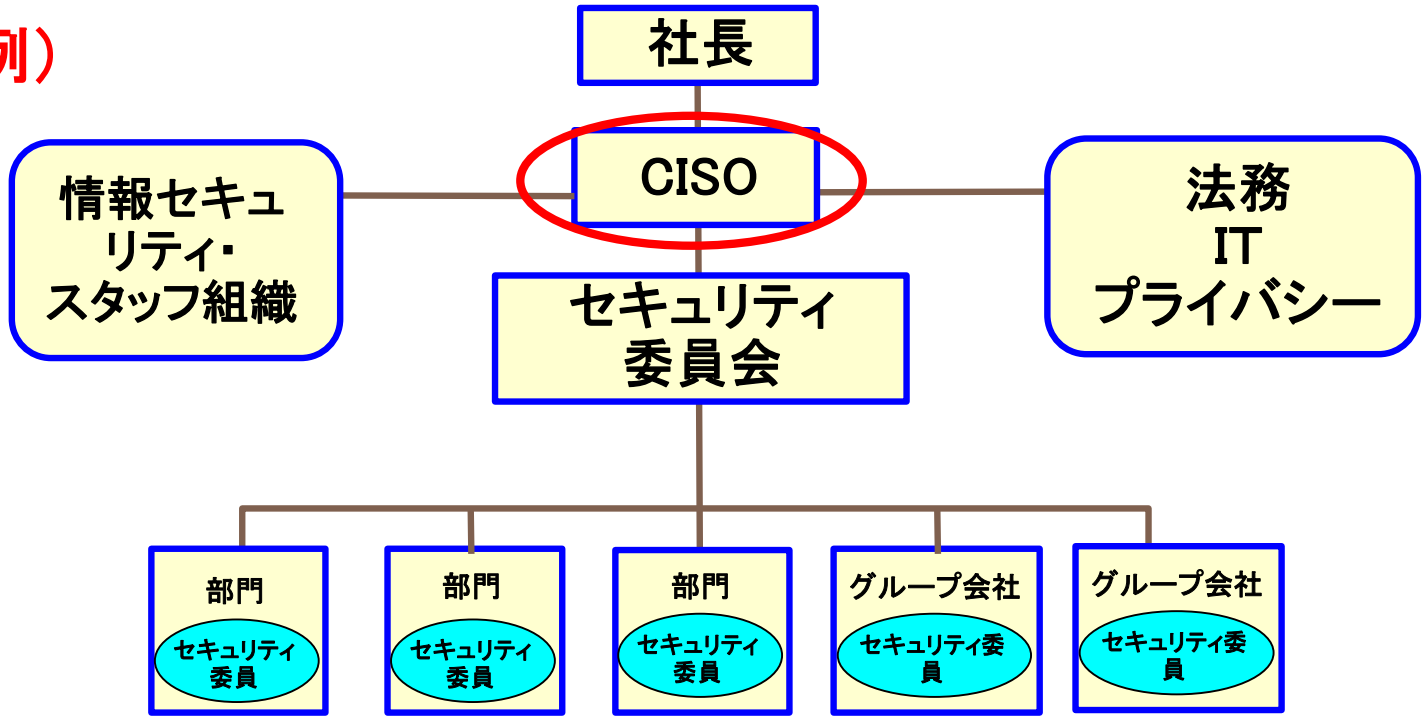


# (1)情報セキュリティマネジメントシステム（ISMS）の基本的要素 – 情報セキュリティを統括するトップマネジメント(CISO) -

■情報セキュリティを統括するトップマネジメント（CISO）の設置

トップマネジメント：最高位(highest level)で組織（Organization）を指揮（Direct）し、管理（Control）する個人又は人々の集まり

（事例）



# (1)情報セキュリティマネジメントシステム（ISMS）の基本的要素 – 適合/不適合と認証制度 -

- 組織のISMSに関して、ISO/IEC 27001 の要求事項に対する「適合」「不適合」が区別できる。

- 認証制度に基づき、認定された第三者機関である審査機関が「適合」を確認することにより、認証が付与される。

  https://www.isms.jipdec.or.jp/isms.html

  – 日本では、日本情報経済社会推進協会 (JIPDEC) で5000超のISMS認証登録

# (2) Integrated Management Systems Standards(IMSS)の適用に関する考え方

- ISO TMB/JTCGが、組織にImplementされている複数のMSSの統合した適用に関するガイドラインが、2017年8月に各TC/SCに送付され、レビューコメントが求められた。
- 複数のMSSとは、例えば、一つの組織に、ISMSとQMS等の他のMSが、構築されているような場合で、その場合、組織・要員、プロセス、規程、手順、システム等、同一組織内で最適化して、Implementする。

| | ISMS | QMS | EMS | xMS |
|---|---|---|---|---|
| 組織・要員 | X | X | Z | X |
| プロセス | X | Y | Z | X |
| 規程 | X | Y | Z | X |
| 手順 | X | Y | Z | X |
| システム | X | Y | Z | X |

# ご説明内容

1. **単一組織の情報セキュリティマネジメントシステム（ISMS）**
   - (1) 情報セキュリティマネジメントシステム（ISMS）の基本的要素
   - (2) Integrated Management Systems Standards(IMSS)の適用に関する考え方

2. **クラウドサービスセキュリティ環境におけるISMS適用の考え方**
   - (1) クラウドサービスセキュリティ環境におけるISMSの構造
   - (2) 局面毎のISMSの役割と機能
     - 局面１：クラウドサービス合意
     - 局面２：情報セキュリティ方針設定
     - 局面３：情報セキュリティ目的/目標の設定
     - 局面４：リスクマネジメントの実施
     - 局面５：管理策の導入と運用
     - 局面６：監視・測定・分析・評価の実施
3. **サイバーセキュリティ環境におけるMS適用の考え方**
   - (1) サイバーセキュリティ環境におけるMSの構造
   - (2) 局面毎のMSの役割と機能
     - 局面１：サイバー空間使用ルールの合意
     - 局面２：サイバーセキュリティ方針設定
     - 局面３：サイバーセキュリティ目的/目標の設定
     - 局面４：リスクマネジメントの実施

# (1)クラウドサービスセキュリティ環境における ISMSの構造

**単一の組織のISMS**

ISMSは、単一組織の情報セキュリティのマネジメントシステム
(27001（規格本文＋附属書 A)

---

## クラウドサービス環境では2組織のISMS

**クラウドサービスカスタマ（CSC）の**
ISMS
(27001（規格本文＋附属書 A)
+27017(CSC))

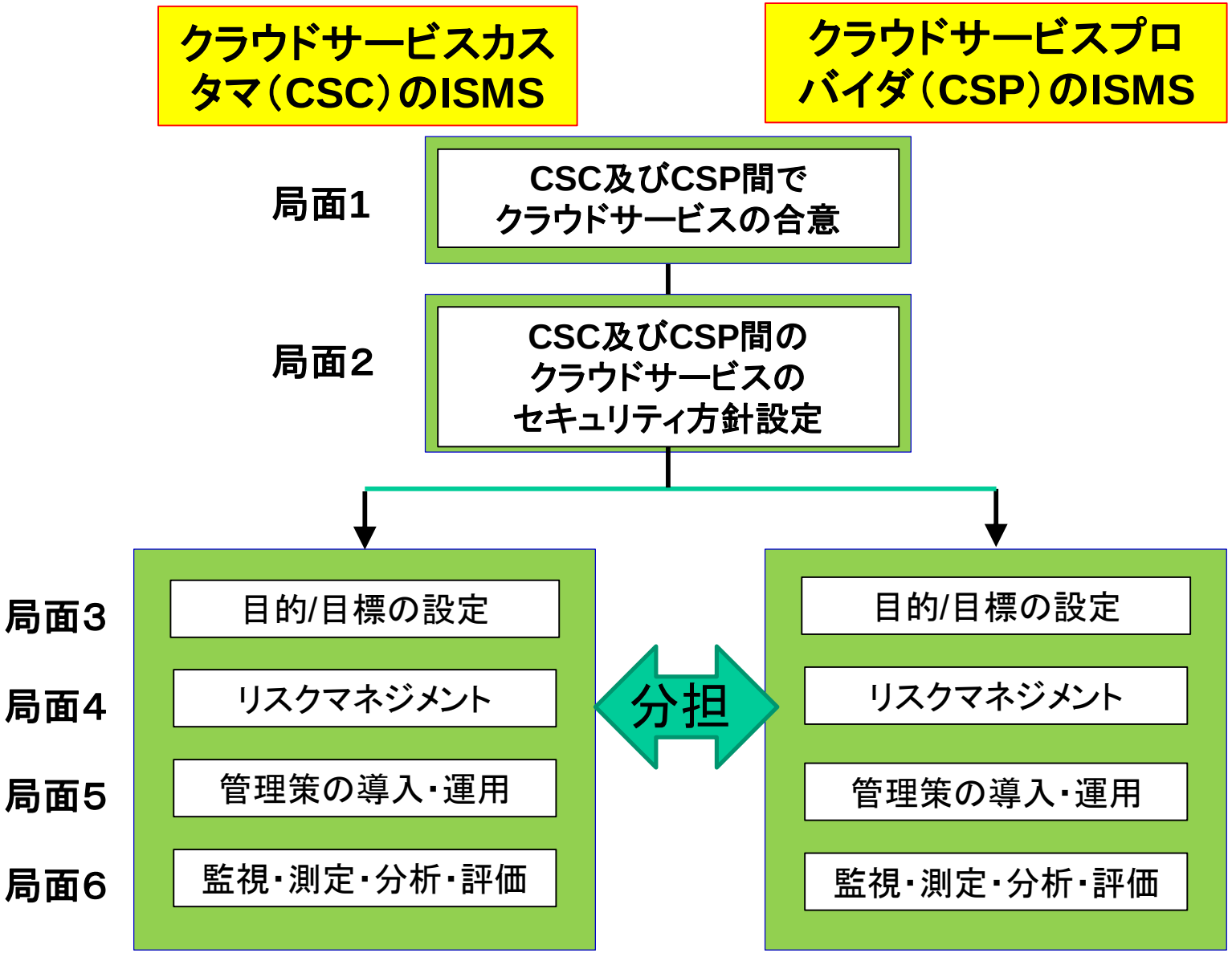
⇔ 分担

**クラウドサービスプロバイダ（CSP）の**
ISMS
(27001（規格本文＋附属書 A)
+27017(CSP))

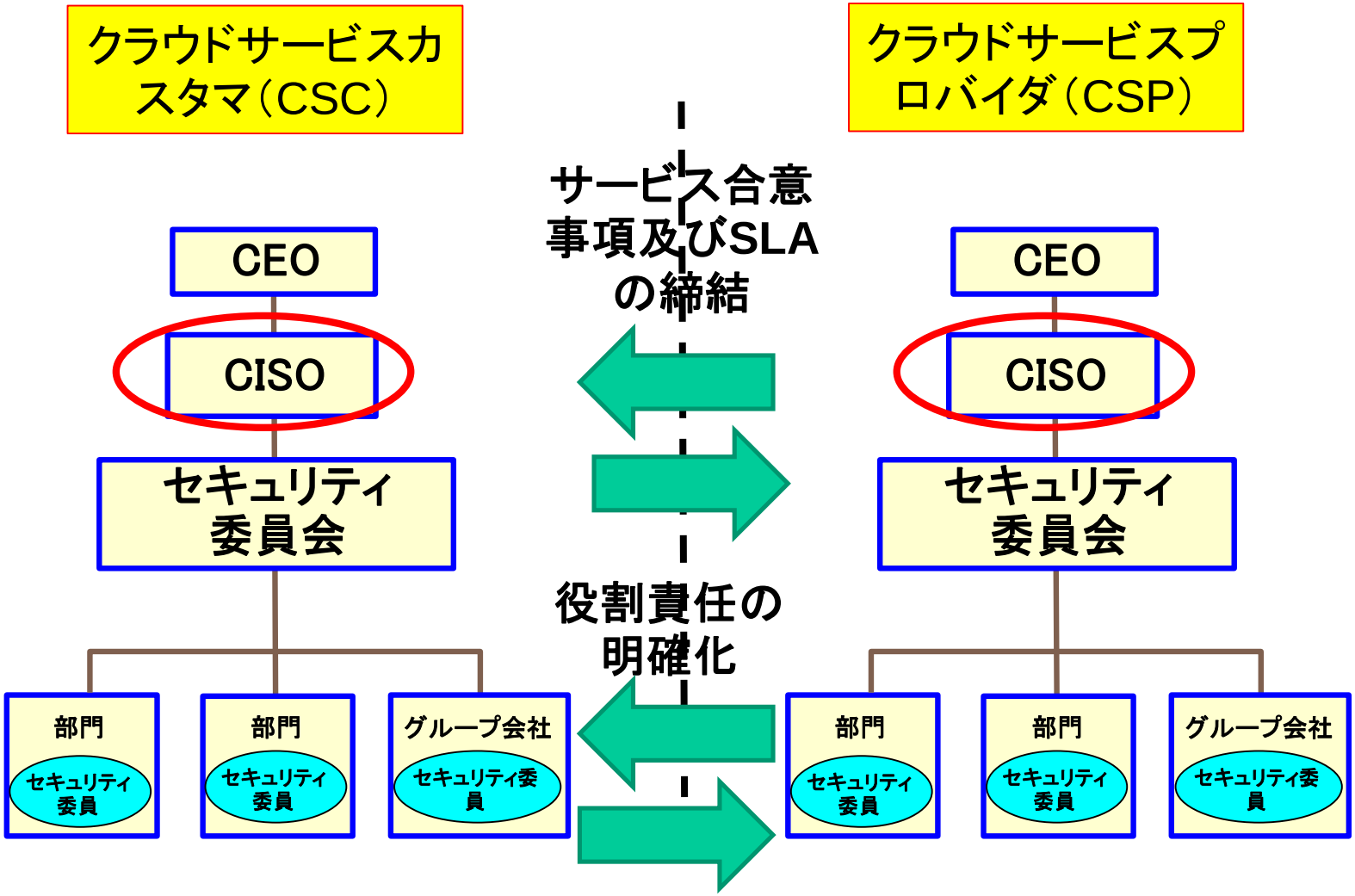
# ご説明内容

1. **単一組織の情報セキュリティマネジメントシステム（ISMS）**
   - (1) 情報セキュリティマネジメントシステム（ISMS）の基本的要素
   - (2) Integrated Management Systems Standards(IMSS)の適用に関する考え方
2. **クラウドサービスセキュリティ環境におけるISMS適用の考え方**
   - (1) クラウドサービスセキュリティ環境におけるISMSの構造
   - (2) 局面毎のISMSの役割と機能
     - 局面１：クラウドサービス合意
     - 局面２：情報セキュリティ方針設定
     - 局面３：情報セキュリティ目的/目標の設定
     - 局面４：リスクマネジメントの実施
     - 局面５：管理策の導入と運用
     - 局面６：監視・測定・分析・評価の実施
3. **サイバーセキュリティ環境におけるMS適用の考え方**
   - (1) サイバーセキュリティ環境におけるMSの構造
   - (2) 局面毎のMSの役割と機能
     - 局面１：サイバー空間使用ルールの合意
     - 局面２：サイバーセキュリティ方針設定
     - 局面３：サイバーセキュリティ目的/目標の設定
     - 局面４：リスクマネジメントの実施

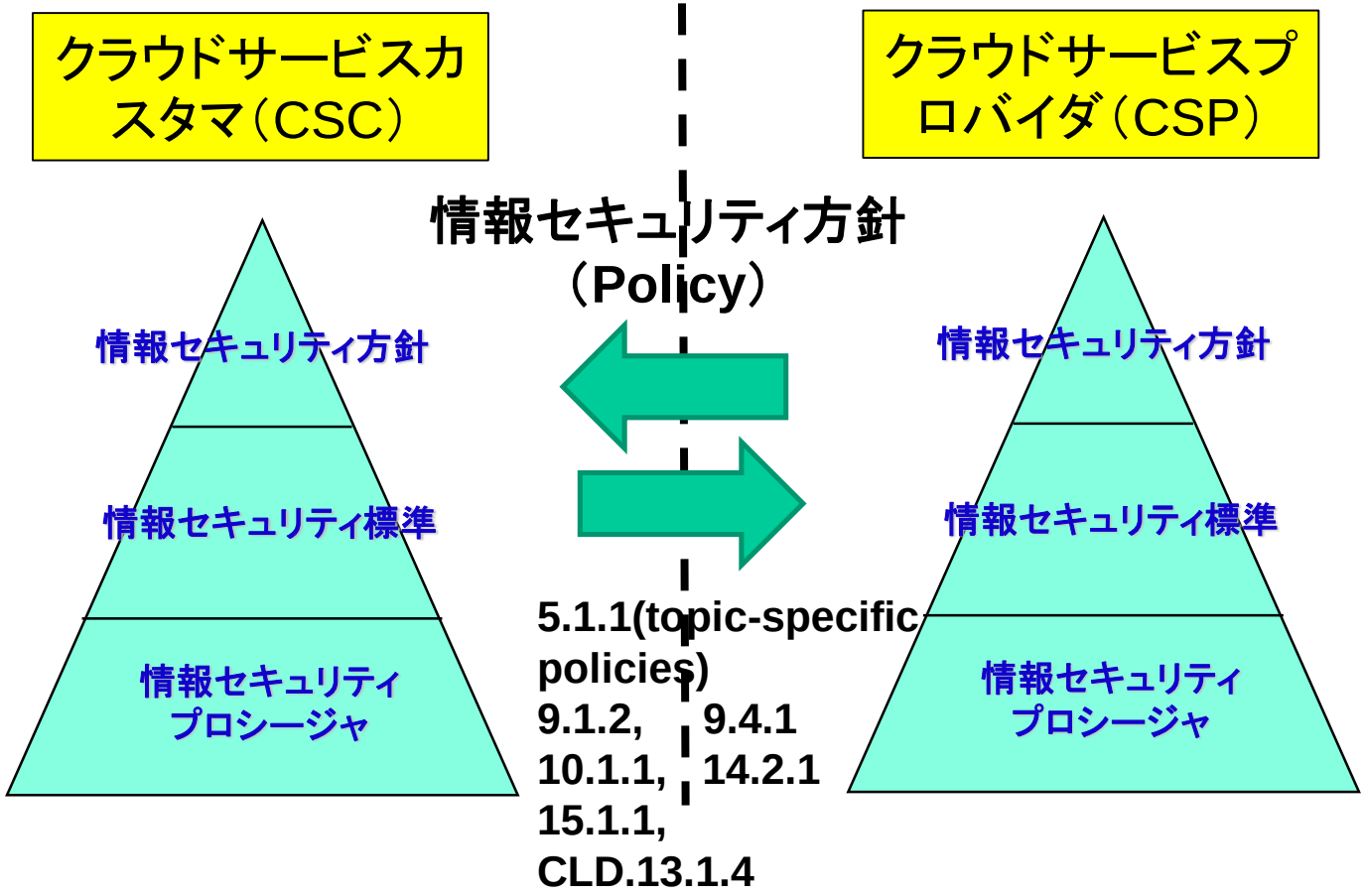
# クラウドサービスにおけるISMSは、ISMSの六つの局面毎にCSCとCSPが分担して実施されます



# 局面1.クラウドサービス合意におけるISO/IEC 27017の活用
## - サービス合意、SLA及び役割と責任 -

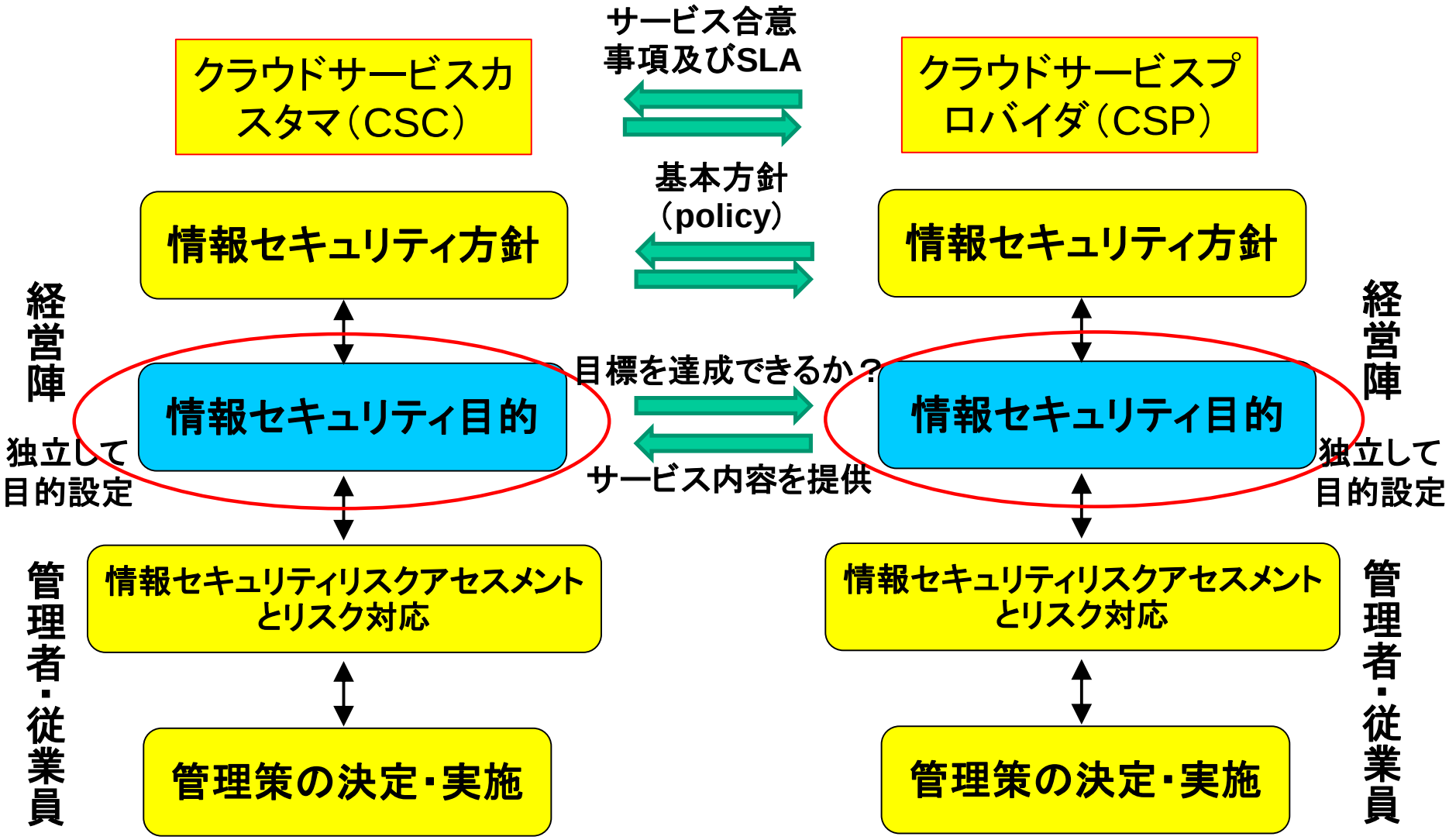


# 局面2.クラウドサービスの情報セキュリティ方針設定における ISO/IEC 27017の活用 - 情報セキュリティ規定体系 -



# 局面3:情報セキュリティ目的/目標の設定における ISO/IEC 27017の活用

- 情報セキュリティ目的はセキュリティ対策の原点です -



# 局面3:情報セキュリティ目的/目標の設定

- 情報セキュリティ目的はセキュリティ対策の原点です -

**事業組織全体としての目的**

- **お客様に影響するインシデントを減らしクラウドサービス事業の信頼性を確保する**

**営業部門の目的**

- お客様情報を含む営業社員のパソコンの紛失インシデントの減少

**クラウドサービス事業部門の目的**

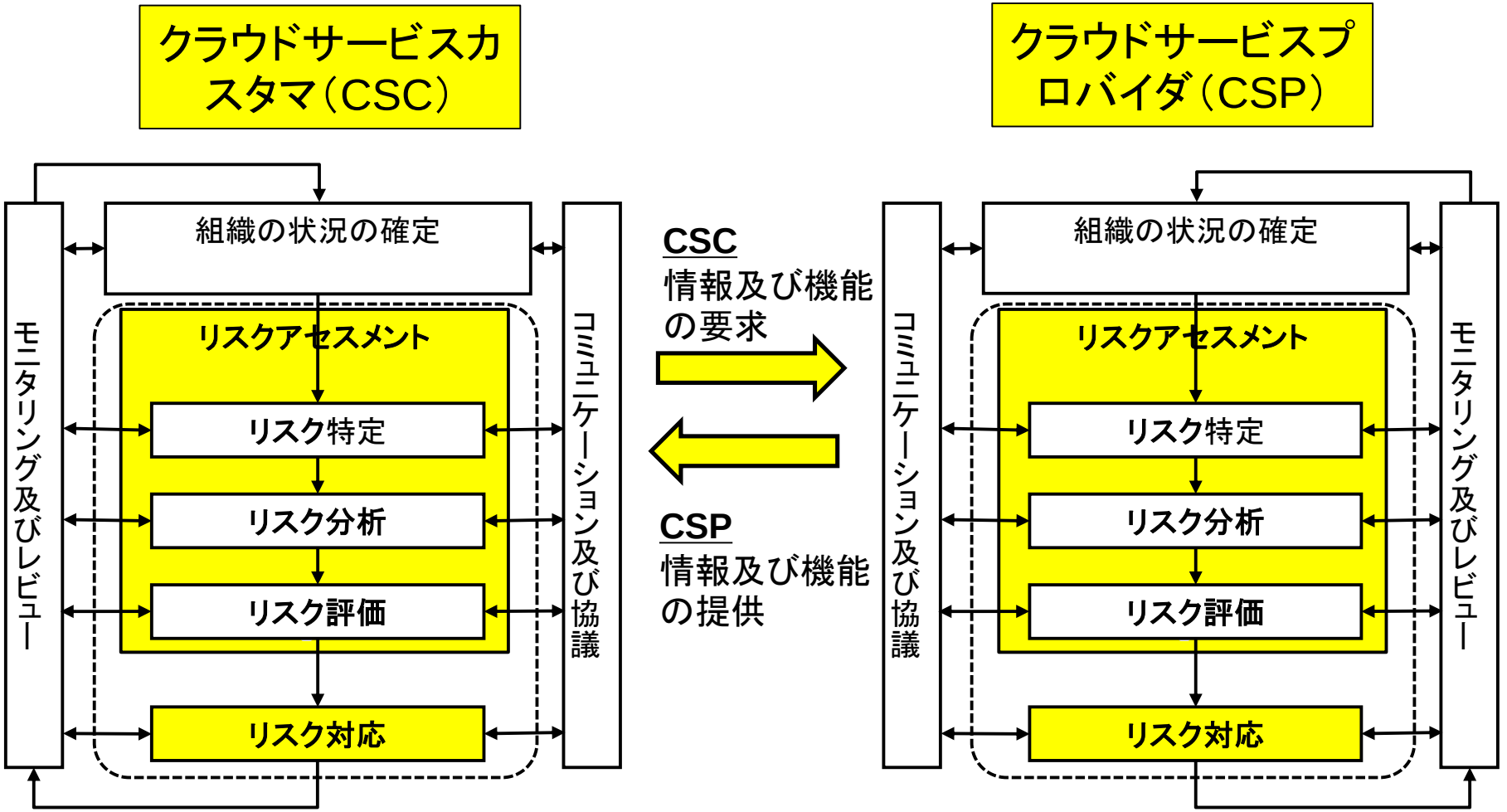
- お客様サービス提供前に必ずSLAを締結

15.1.3ICTサプライチェーンの管理策を適用

**データセンター運営会社の目的**

- システム要因による顧客に影響するインシデントの減少

# 局面4:リスクマネジメントの実施
## - リスクアセスメント(リスク特定、リスク分析、リスク評価)-



# 局面4:リスクマネジメントの実施における ISO/IEC 27017の活用

- リスクアセスメント、リスク対応の事例-

**リスクの定義＝目的に対する不確かさの影響**

クラウドサービスプロバイダのデータセンターの事例

*目的に影響を与えるリスク因子*

**リスク源** Vendor lock-in

**CSP側のケース (データセンター)**

**情報セキュリティ目的**

**CIAレベル**

**情報のCIAの喪失**

**結果(Consequence)**

*目的に影響を与える事象の結末*

- データセンターにおけるシステム要因によるクラウドサービス事業の顧客に影響するインシデントの減少 *(前年比50％)*

**事象と原因** バックアップを取得していたが、リストアしたが使用できなかった

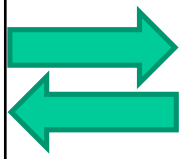
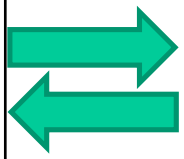
*ある一連の周辺状況の出現又は変化*

**起こりやすさ(likelihood)**

*何かが起こる可能性*

(インパクトはAvailability)お客様から預かったお客様情報を紛失し、しかも、バックアップを取得していたが、使用できなかった。お客様の事業を継続できず、場合により損害賠償

# 局面4:リスクマネジメントの実施
## - リスクアセスメントの連携の事例-

| CSC/CSP | クラウドサービスカスタマ（CSC） | 分担 | クラウドサービスプロバイダ(データセンター)(CSP) |
|---|---|---|---|
| 情報セキュリティ目的 | サービスの使用可能性(Availability)を基準(Criteria)以上とする | | システム要因によるクラウドサービス事業の顧客に影響するインシデントの減少 |
| リスクアセスメント対象 | 異なるサービス間の整合性（データ破壊したクラウドの使用を中止して別システムに移行。取っていたバックアップデータを使用して、システムの継続を実施） | | |
| 事象 | ①データ破壊に依るシステム停止。③バックアップデータを使用を試みたが使用できなかった |  | ②CSCにバックアップデータを提供した。④（CSCよりの連絡）CSCのシステムで、利用できない |
| リスク源 | アクセス制御不備、バックアップテストの未テスト |  | バックアップデータに、特定の開発業者のソフトウェアを含んでいる(Vendor lock-in) |
| 結果 | CSCがシステムの使用ができず、結果的にサービスの利用停止となった。 | | CSPが提供するシステムにおいてシステム停止が発生し、再開ができない。 |

# 局面5:管理策の導入・運用における ISO/IEC 27017の活用

## - リスク対応による管理策の導入と運用 -

ISO/IEC27002(27017)の管理策＋ISO/IEC27002+27017の実施の手引

**12.3.1:** 情報，ソフトウェア及びシステムイメージのバックアップは，合意されたバックアップ方針に従って定期的に取得し，検査することが望ましい。

**CSCのバックアップ方針**

- バックアップ機能仕様要求
- バックアップ取得
- 取得バックアップの検査
- 要求事項充足の検査

**CSPのバックアップ方針**

- バックアップ取得
- 取得バックアップの検査

**CSCへのバックアップ支援方針**

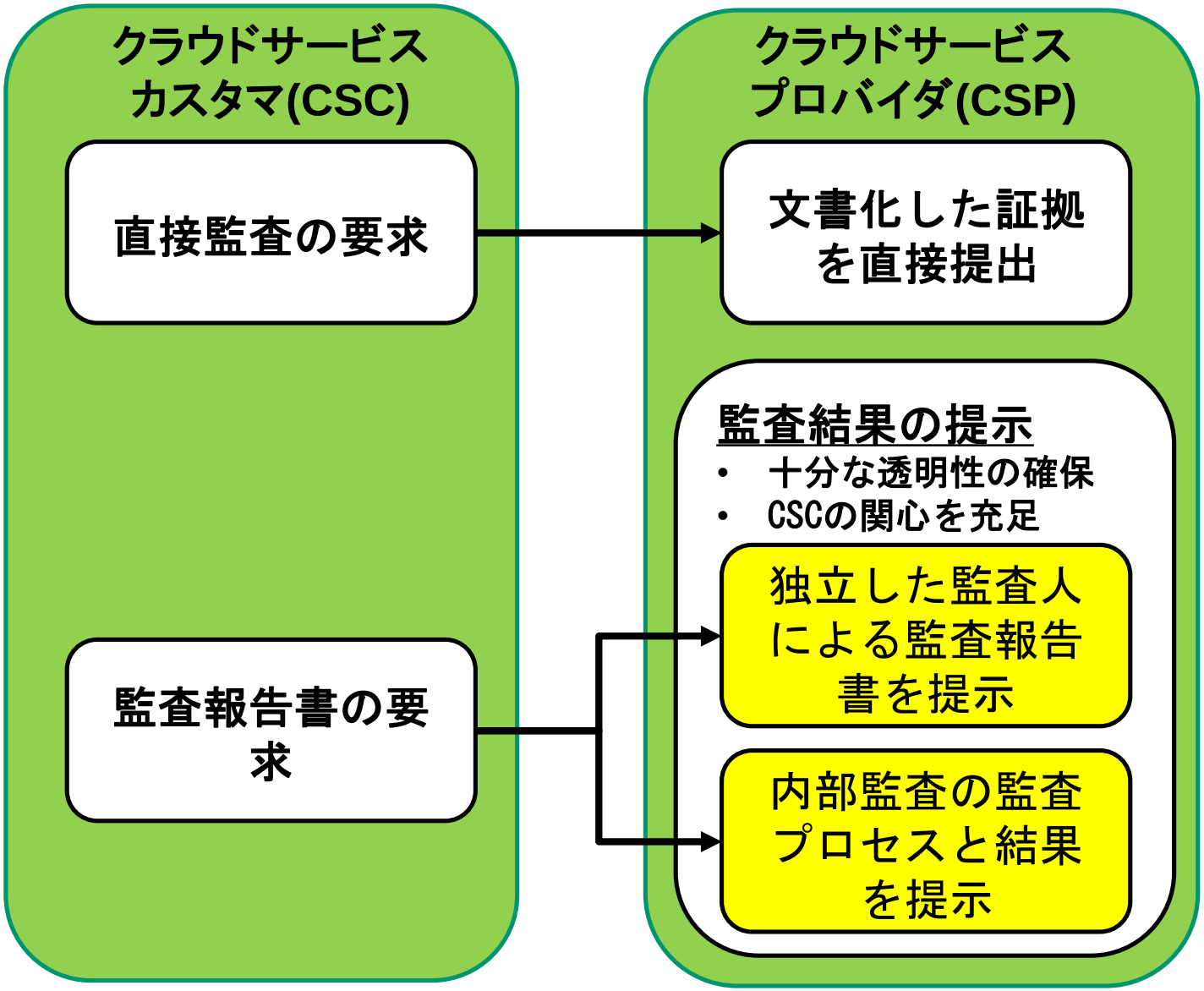
- バックアップ機能仕様提供

**要求事項充足状況に基づく方針見直しの検討**

**二組織が連携したバックアップ方針**

# 局面6:監視・測定・分析・評価の実施

- CSCは、信頼できるCSPの監査情報を把握できないとセキュリティ対策はできない -



# ご説明内容

1. **単一組織の情報セキュリティマネジメントシステム（ISMS）**
   - (1) 情報セキュリティマネジメントシステム（ISMS）の基本的要素
   - (2) Integrated Management Systems Standards(IMSS)の適用に関する考え方
2. **クラウドサービスセキュリティ環境におけるISMS適用の考え方**
   - (1) クラウドサービスセキュリティ環境におけるISMSの構造
   - (2) 局面毎のISMSの役割と機能
     - 局面１：クラウドサービス合意
     - 局面２：情報セキュリティ方針設定
     - 局面３：情報セキュリティ目的/目標の設定
     - 局面４：リスクマネジメントの実施
     - 局面５：管理策の導入と運用
     - 局面６：監視・測定・分析・評価の実施
3. **サイバーセキュリティ環境におけるMS適用の考え方**
   - (1) サイバーセキュリティ環境におけるMSの構造
   - (2) 局面毎のMSの役割と機能
     - 局面１：サイバー空間使用ルールの合意
     - 局面２：サイバーセキュリティ方針設定
     - 局面３：サイバーセキュリティ目的/目標の設定
     - 局面４：リスクマネジメントの実施

## (1) サイバーセキュリティ環境におけるマネジメントシステム（MS）の構造 - サイバーセキュリティの定義 -

SC27会議（ベルリン）の事前に9通りの定義案があり、結論は出ていないが、活発な議論が進んでいる

- 「サイバー空間」における「情報セキュリティの維持」だけでなく、「サイバー攻撃に対処する」も含めて、「デジタル化社会のリスクへの対応」

  例：safeguarding of society, people, organization and nation from digital risks

- 組織や個人の情報セキュリティとしての自衛の手段としてだけでなく、共有財産である「サイバー空間の安全確保」が必要。すなわち、「情報システムやIoT機器の適正な維持が必要」

  例：protection of systems, networks and data in cyberspace

# (1) サイバーセキュリティ環境におけるマネジメントシステム（MS）の構造 - サイバーセキュリティの定義 -

まだ結論は出ていないが、以下の方向で、活発な議論が進んでいる – (続き）

- 「サイバー空間」のインフラにおいて、共有財産である「サイバー空間の安全確保」に関しては、不正検知、強固なDNS設定等の技術的対策と、脆弱性情報・攻撃情報の共有等の制度・運用の強化が考えられる
- 「誰にとっての安全か、誰が施策を担うのか」などのサイバー空間に関わる各当事者を明確にすることが重要と考える

# (1) サイバーセキュリティ環境におけるマネジメントシステム（MS）の構造 - サイバーセキュリティの定義 -

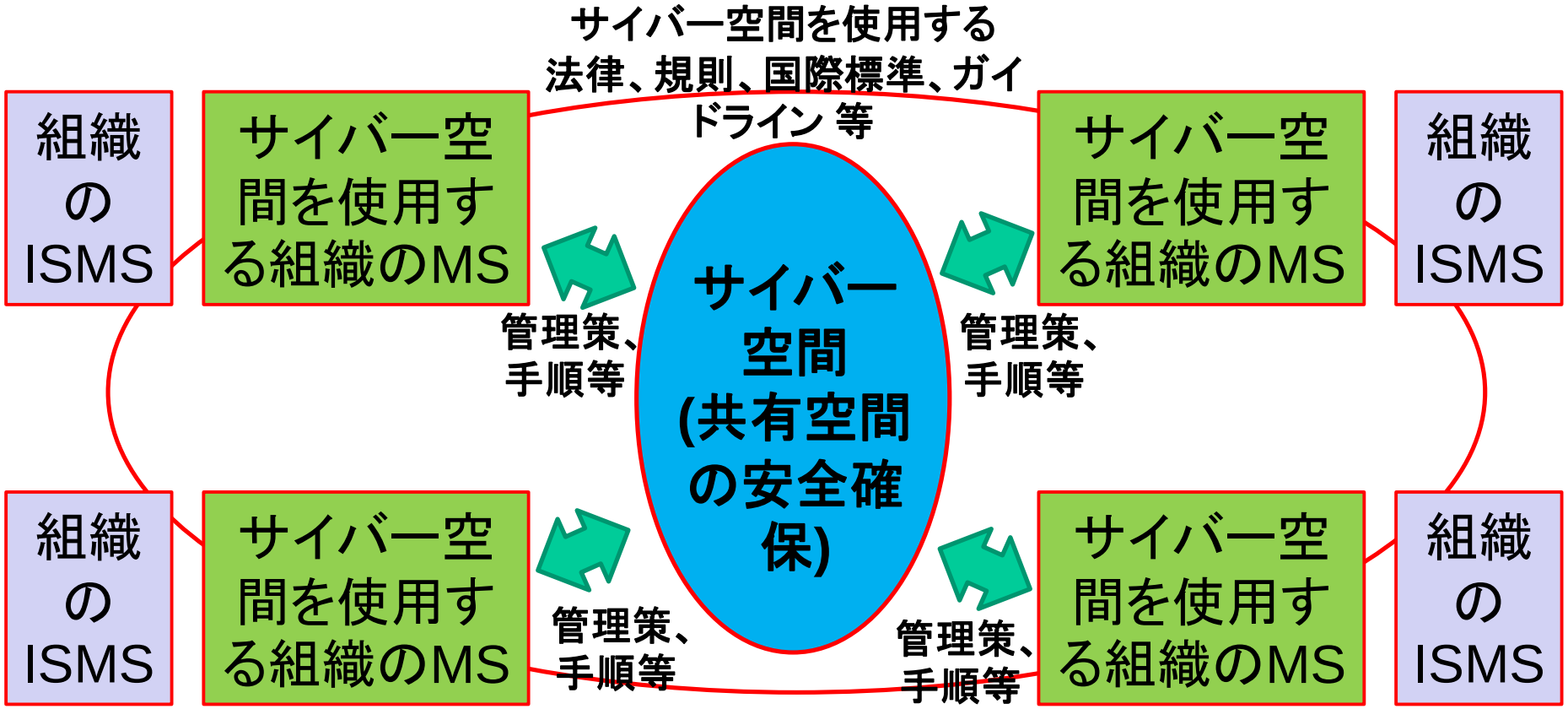
「サイバーセキュリティの定義」から対象者に着目して整理すると

- ISMSの基本形では
  - ✓ 一組織の情報セキュリティを扱う
  - ✓ 情報セキュリティ(information security): preservation of confidentiality, integrity and availability of information
- サイバーセキュリティでは
  - ✓ 多数の当事者が関わる「サイバー空間」を前提に考えることが多い

# (1) サイバーセキュリティ環境におけるマネジメントシステム（MS）の構造

**サイバーセキュリティ環境におけるMSの目的と方針、**

- **組織の共有空間であるサイバー空間の安全確保、及び**
- **社会、国民、組織、国家 (**society, people, organization, nation)を**サイバーアタックからの防御**

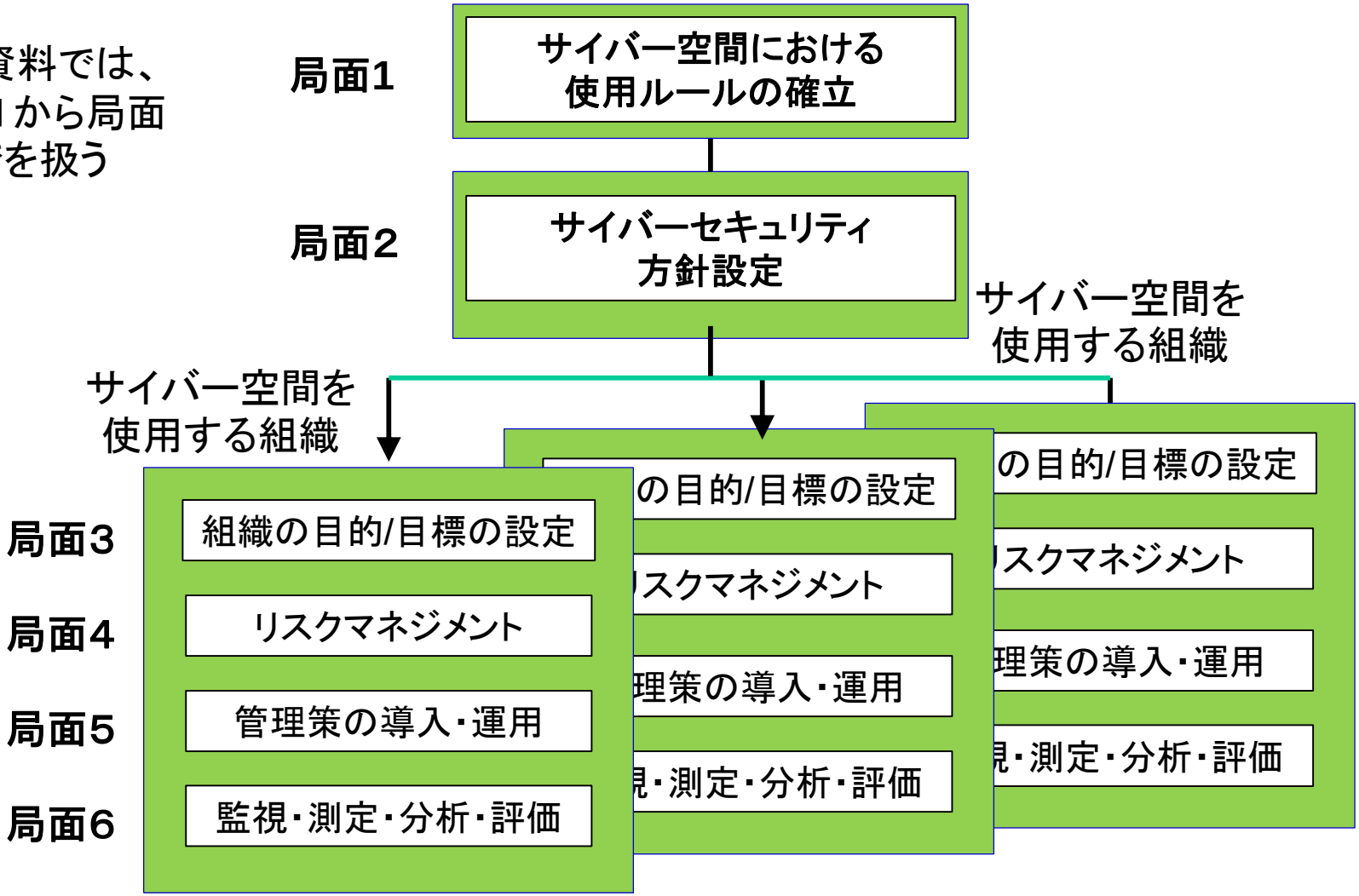


# ご説明内容

1. **単一組織の情報セキュリティマネジメントシステム（ISMS）**
   - (1) 情報セキュリティマネジメントシステム（ISMS）の基本的要素
   - (2) Integrated Management Systems Standards(IMSS)の適用に関する考え方
2. **クラウドサービスセキュリティ環境におけるISMS適用の考え方**
   - (1) クラウドサービスセキュリティ環境におけるISMSの構造
   - (2) 局面毎のISMSの役割と機能
     - 局面１：クラウドサービス合意
     - 局面２：情報セキュリティ方針設定
     - 局面３：情報セキュリティ目的/目標の設定
     - 局面４：リスクマネジメントの実施
     - 局面５：管理策の導入と運用
     - 局面６：監視・測定・分析・評価の実施
3. **サイバーセキュリティ環境におけるMS適用の考え方**
   - (1) サイバーセキュリティ環境におけるMSの構造
   - (2) 局面毎のMSの役割と機能
     - 局面１：サイバー空間使用ルールの合意
     - 局面２：サイバーセキュリティ方針設定
     - 局面３：サイバーセキュリティ目的/目標の設定
     - 局面４：リスクマネジメントの実施

# サイバーセキュリティ環境におけるMSは、サイバー空間の使用組織が、安全にサイバー空間を共同で使用できるように、MSの6局面に沿って実施します

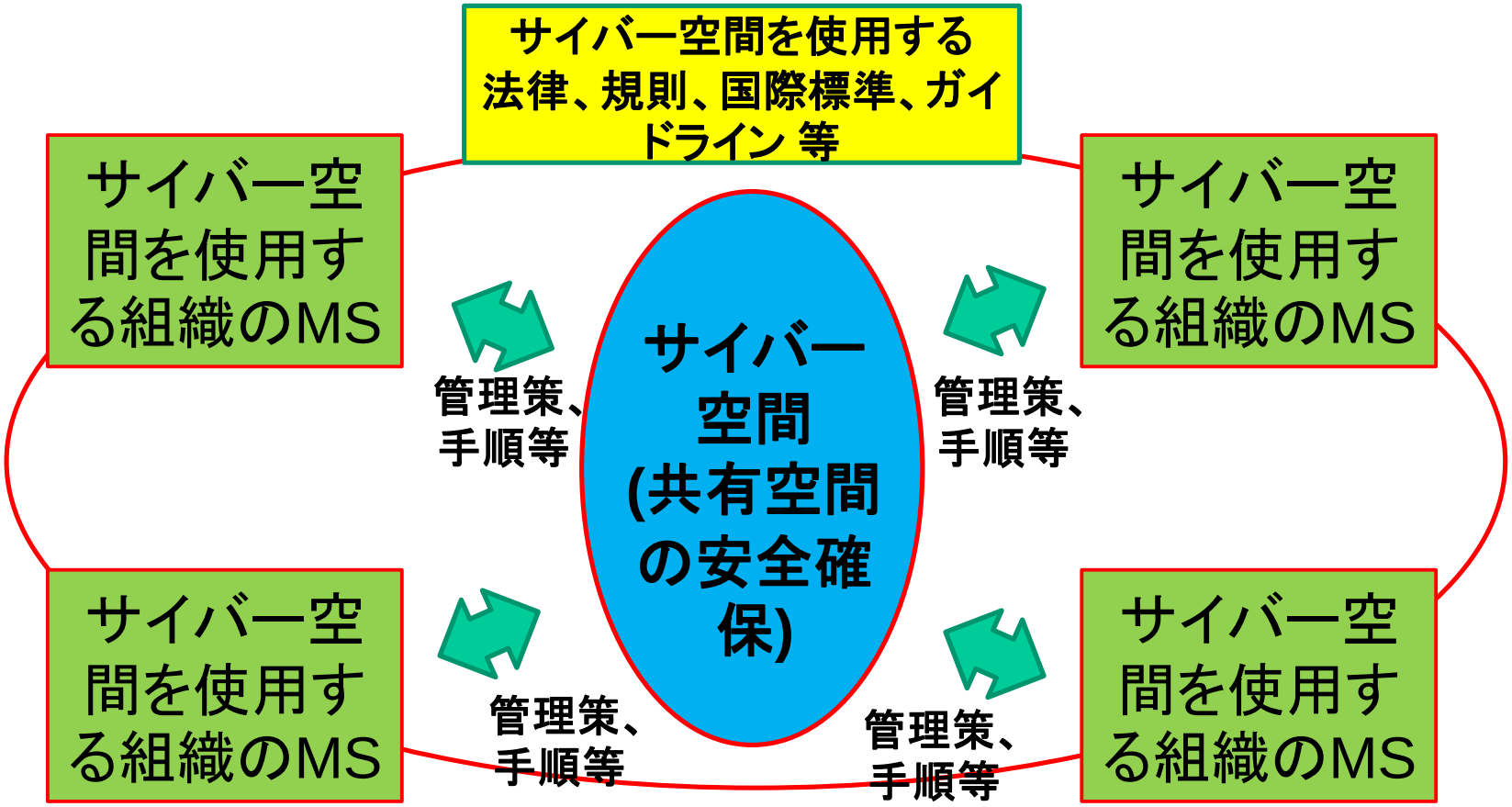
（注）
この資料では、局面1から局面4までを扱う



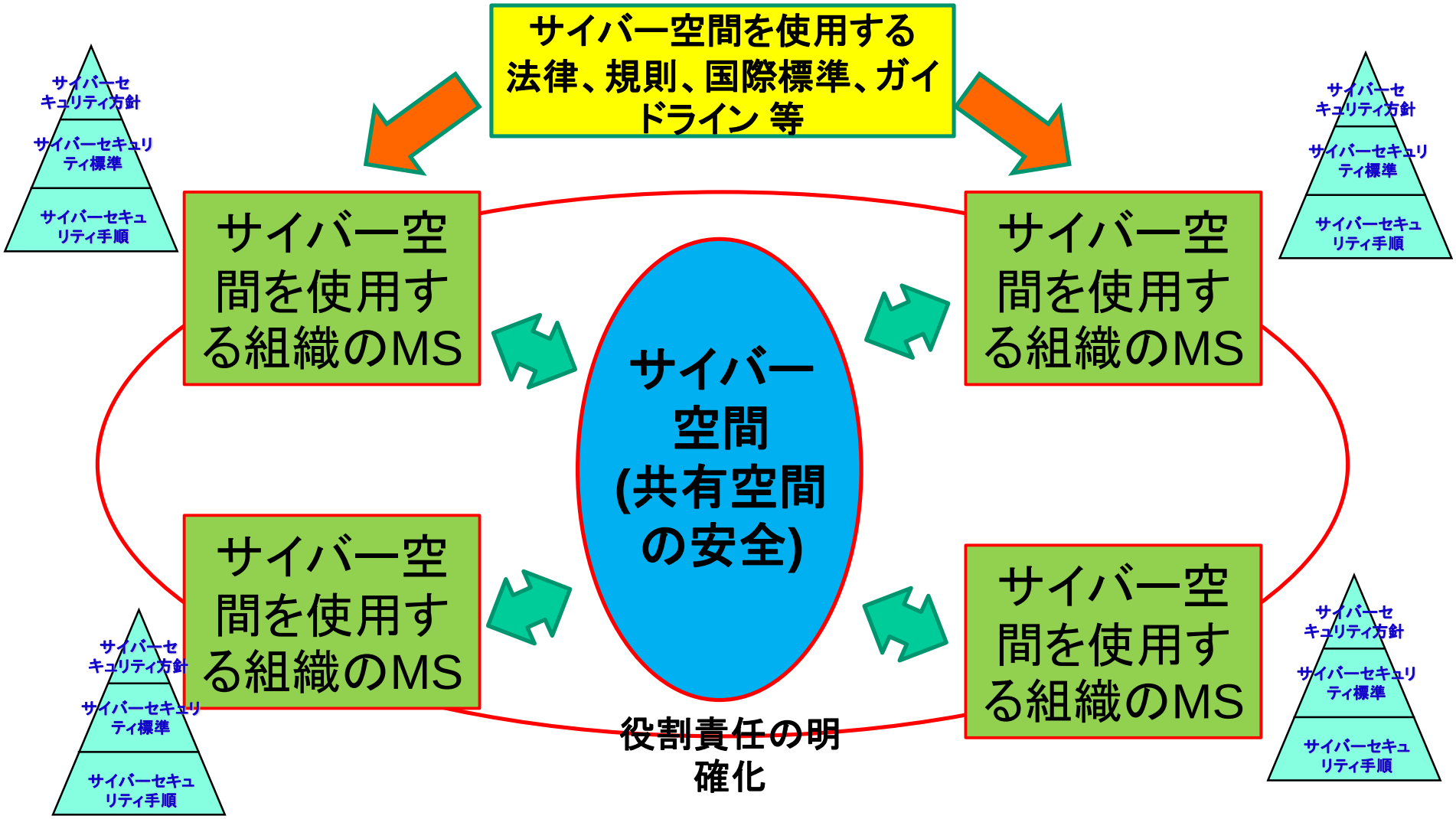
# 局面1.サイバー空間における使用ルール
## - 使用ルールに関する法律,規則,国際標準,ガイドライン等 -

**サイバーセキュリティ環境におけるMSの目的と方針、**

- **組織の共有空間であるサイバー空間の安全確保、及び**
- **社会、国民、組織、国家 (**society, people, organization, nation)を**サイバーアタックからの防御**

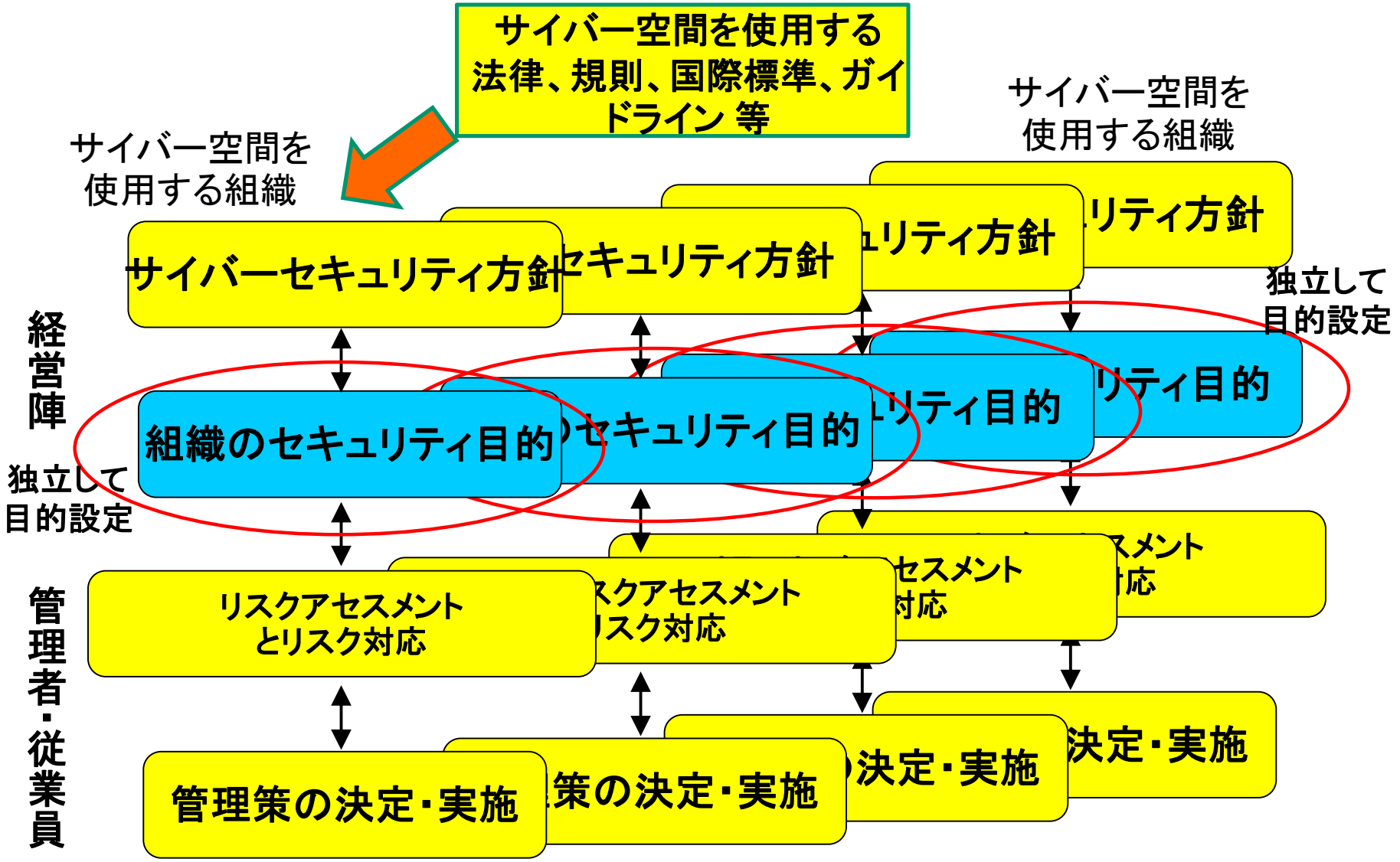


# 局面2.サイバーセキュリティ環境におけるサイバーセキュリティ方針設定
## - 各使用組織のサイバーセキュリティ規定体系 -



# 局面3：サイバーセキュリティ目的/目標の設定

- サイバーセキュリティ目的はセキュリティ対策の原点です -



# 局面3：サイバーセキュリティ目的/目標の設定

- 組織のサイバーセキュリティ目的はセキュリティ対策の原点です -

**使用組織全体としての目的**

- （例）共有財産であるサイバー空間使用に関するインシデントを発生させない。そのための方針・ガイドラインを出す

**サイバー空間の使用部門（営業）の目的**

- （例）サイバー空間を使用してのお客様情報の紛失インシデントの減少

**サイバー空間の直接運用管理部門の目的**

- （例）運用管理によりサイバー空間を使用しての他の組織に影響を与えるインシデントを発生させない

（例）

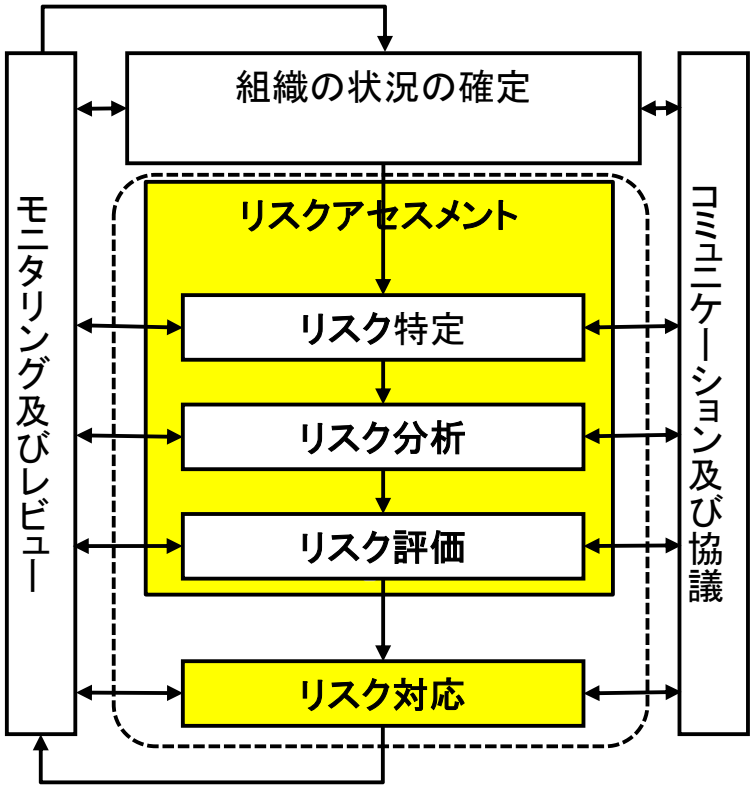
1. 当組織からサイバー空間を使用する場合、ネットワーク要因による他の組織に影響を与えるインシデントの減少
2. 当組織からサイバー空間を使用する場合、運用管理要因による他の組織に影響を与えるインシデントの減少

# 局面4:リスクマネジメントの実施

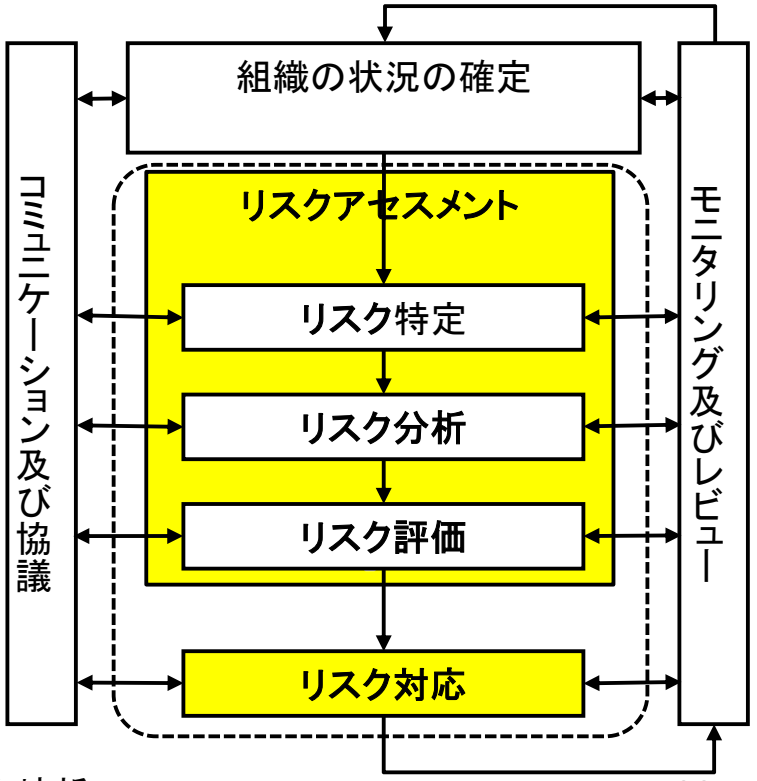
## - リスクアセスメント(リスク特定、リスク分析、リスク評価)-

法律、規則、国際標準、
ガイドライン 等

サイバー空間を使用する組織

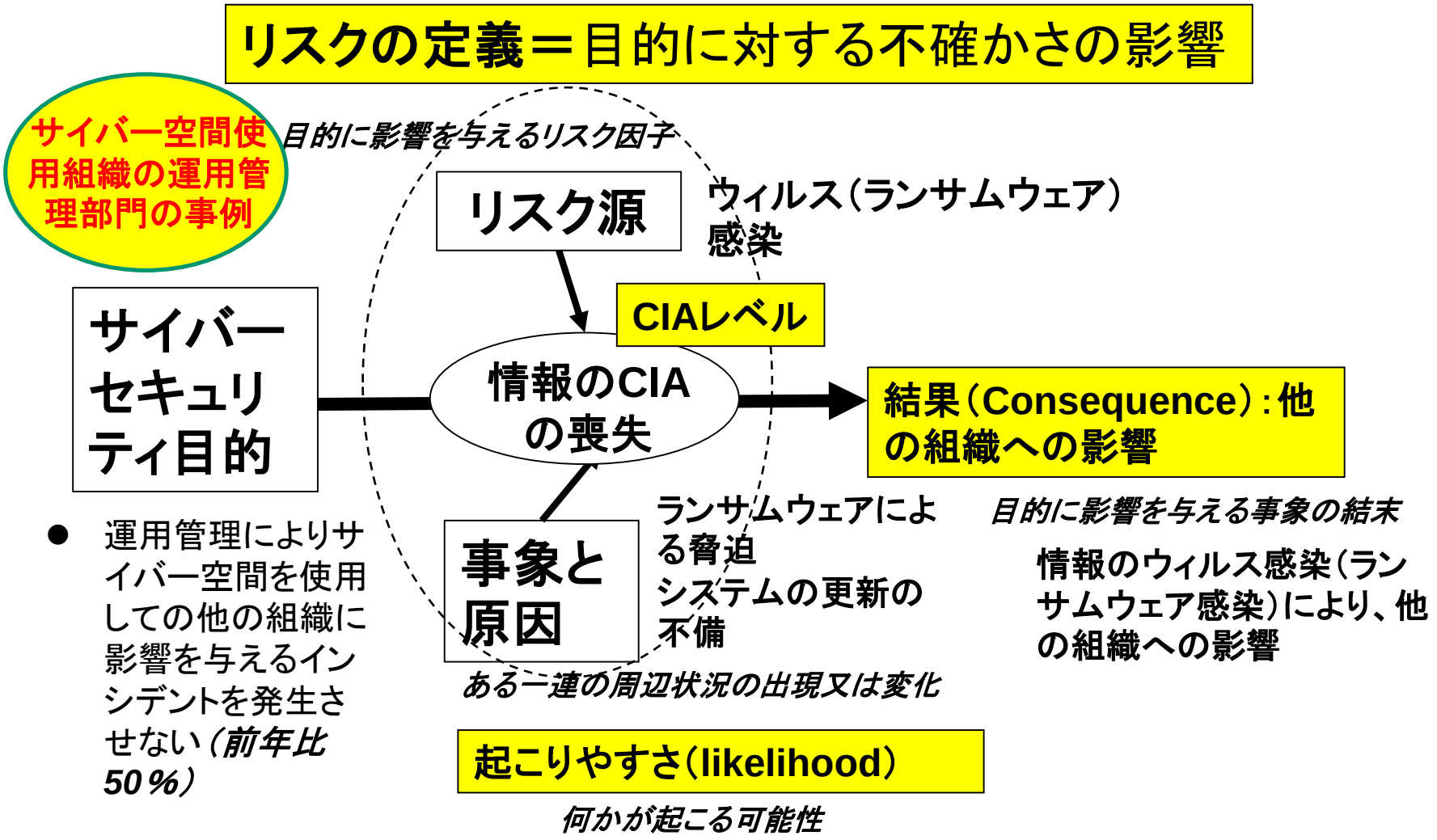



サイバー空間を使用する組織



# 局面4:リスクマネジメントの実施

## - リスクアセスメント、リスク対応の事例-




- 運用管理によりサイバー空間を使用しての他の組織に影響を与えるインシデントを発生させない（*前年比50％*）

# おわりに

## ご清聴有難うございました。

工学院大学情報学部
ISO/IEC JTC1/SC27/WG1主査
やまさき　さとる
山﨑　哲