

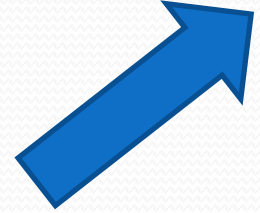
# 事業継続マネジメントシステムによる組織レジリエンスの向上

## － マネジメントシステムとして 取り組む意義 －

株式会社インターリスク総研  
事業リスクマネジメント部 事業継続マネジメントグループ  
(JIPDEC BCMS適合性評価制度 運営委員会 委員)  
田代 邦幸

2014年9月24日

Copyright JIPDEC 2014



画面上のスライドは、  
お手元に配布された資料とは  
若干異なります。



マークがついたスライドは、  
お手元に配布しておりません。

# 今日お話ししたいこと

- 組織レジリエンスの向上に本気で取り組むならば、事業継続マネジメントシステム(BCMS)として取り組まなければならない
- マネジメントシステムとして取り組むためには、ISO22301や、そのガイダンスであるISO22313、JIPDEC BCMSユーザーズガイドを参考にとよい

# 事業継続マネジメントシステムの定義

- マネジメントシステム全体の中で, 事業継続の確立, 導入, 運用, 監視, レビュー, 維持及び改善を担う部分。  
(JIS Q 22301)
- part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity  
(ISO 22301)

# マネジメントシステムの定義

- 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。  
(JIS Q 22301)
- set of interrelated or interacting elements of an organization to establish policies and objectives, and processes to achieve those objectives  
(ISO 22301)

**どんな会社にも大抵ある仕組み**



**マネジメントシステムは  
どこの会社でもある仕組み**



**既に自社にある仕組みを使って  
事業継続力を維持向上  
させていきましょう**

# マネジメントシステム $\neq$ ISO規格で定められている PDCA サイクルに基づく仕組み

世界各国における研究や実践の蓄積を経て、効果的な手法として国際的に認知されているマネジメントシステムの一手法が、ISOのMSS(Management System Standard)

# ISO MSSの統一フォーマット

ISO 22301:2012

・2012年に策定されたMSS(マネジメントシステム規格)の統一フォーマット「上位構造、共通の中核となるテキスト、共通用語及び中核となる定義」のスタイルを用いている



「上位構造、共通の中核となるテキスト、共通用語及び中核となる定義」のスタイルは、「ISO/IEC 専門業務用指針 統合版ISO 補足指針－ISO 専用手順」に2012年5月に追加された「[附属書SL](#)」のAppendix

■[附属書SL](#) = A + B

→位置付けをISOのGuide文書から専門業務用指針の一部に格上げ

A:従来のMSS作成の基本ルールについて示す「ISO Guide 72 マネジメントシステム規格の正当性及び作成に関する指針」

B:要求事項規格の書き方に関するAppendix

■Appendix2・3・4:

ISOマネジメントシステム“要求事項”規格全てを整合化し、これらの規格の両立性を向上させることを目的とし、要求事項規格共通の構成を示す。

■Appendix3

具体的な構造とMSS全般に共通する要素に関する文面のフォーマット並びに用語の定義について「上位構造、共通の中核となるテキスト、共通用語及び中核となる定義」を示している。

附属書SLの背景

・これまで策定された30以上のMSSの構成に統一性がない。

→例:9001、14001、27001の章立ての時点で既に構成が異なっている。

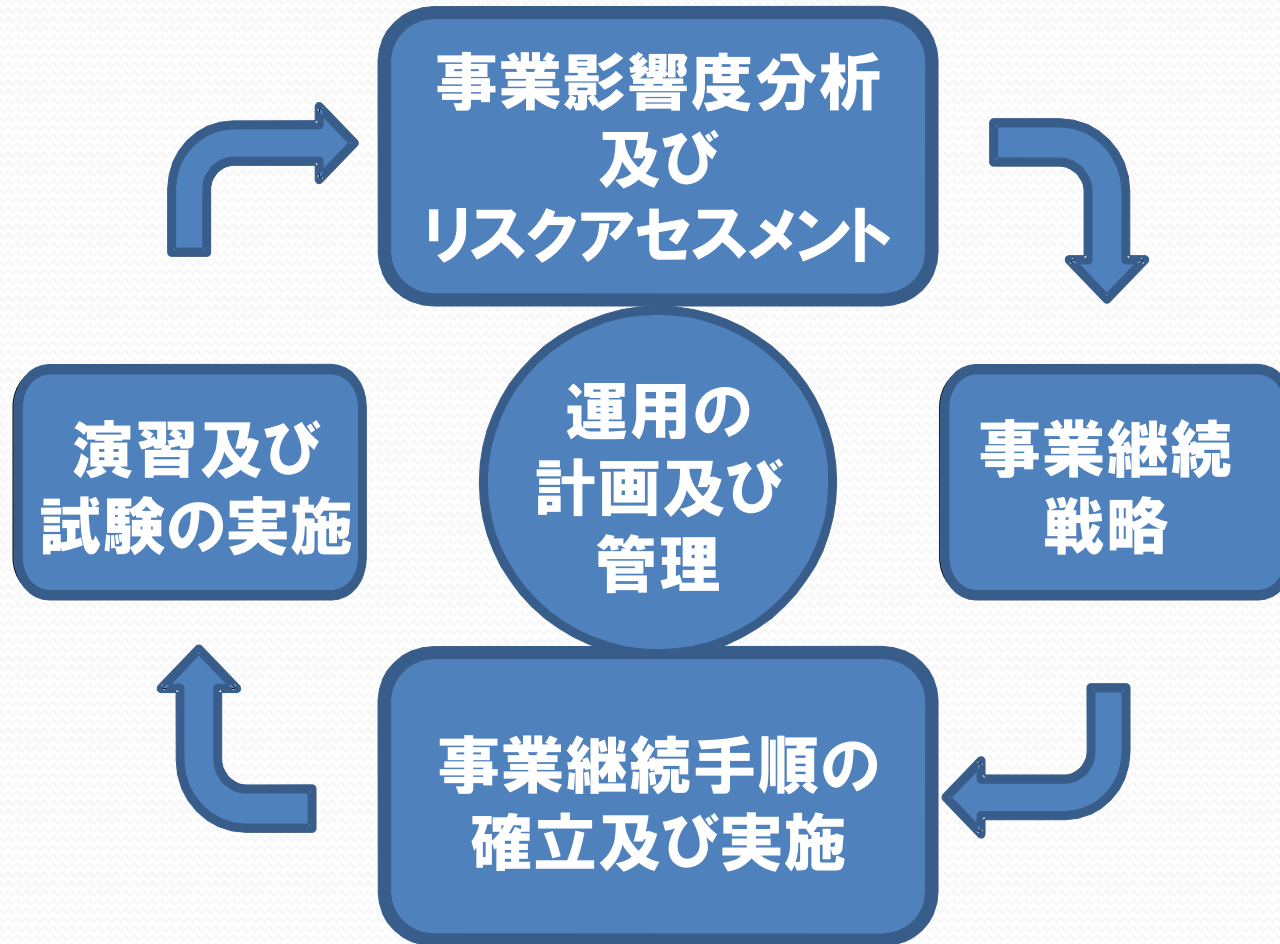
| 章  | 項    | タイトル                  | PDCA |
|----|------|-----------------------|------|
| 0  |      | 序文                    | —    |
|    | 0.1  | 一般                    |      |
|    | 0.2  | PDCAモデル               |      |
|    | 0.3  | この国際規格におけるPDCAの構成要素   |      |
| 1  |      | 適用範囲                  | P    |
| 2  |      | 引用規格                  |      |
| 3  |      | 用語及び定義                |      |
| 4  |      | 組織の状況                 |      |
|    | 4.1  | 組織とその状況の理解            |      |
|    | 4.2  | 利害関係者のニーズ及び期待の理解      |      |
|    | 4.3  | XXXマネジメントシステムの適用範囲の決定 |      |
|    | 4.4  | XXXマネジメントシステム         |      |
| 5  |      | リーダーシップ               |      |
|    | 5.1  | リーダーシップ及びコミットメント      |      |
|    | 5.2  | 経営者のコミットメント           |      |
|    | 5.3  | 方針                    |      |
|    | 5.4  | 組織の役割、責任及び権限          |      |
| 6  |      | 計画                    | D    |
|    | 6.1  | リスク及び機会に対応するための処置     |      |
| 7  |      | 支援                    |      |
|    | 7.1  | 資源                    |      |
|    | 7.2  | 力量                    |      |
|    | 7.3  | 認識                    |      |
|    | 7.4  | コミュニケーション             |      |
|    | 7.5  | 文書化した情報               |      |
| 8  |      | 運用                    |      |
|    | 8.1  | 運用の計画及び管理             |      |
|    | 8.2  | 事業影響度分析及びリスクアセスメント    |      |
|    | 8.3  | 事業継続戦略                |      |
|    | 8.4  | 事業継続手順の確立及び導入         |      |
| 9  |      | パフォーマンス評価             | C    |
|    | 9.1  | 監視、測定、分析及び評価          |      |
|    | 9.2  | 内部監査                  |      |
|    | 9.3  | マネジメントレビュー            |      |
| 10 |      | 改善                    | A    |
|    | 10.1 | 不適合及び是正処置             |      |
|    | 10.2 | 継続的改善                 |      |

# BCMS $\neq$ ISO22301

ISO22301/22313は、  
世界各国における研究や実践の蓄積を経て、  
効果的な手法として推奨されている  
BCMSへの取り組み方

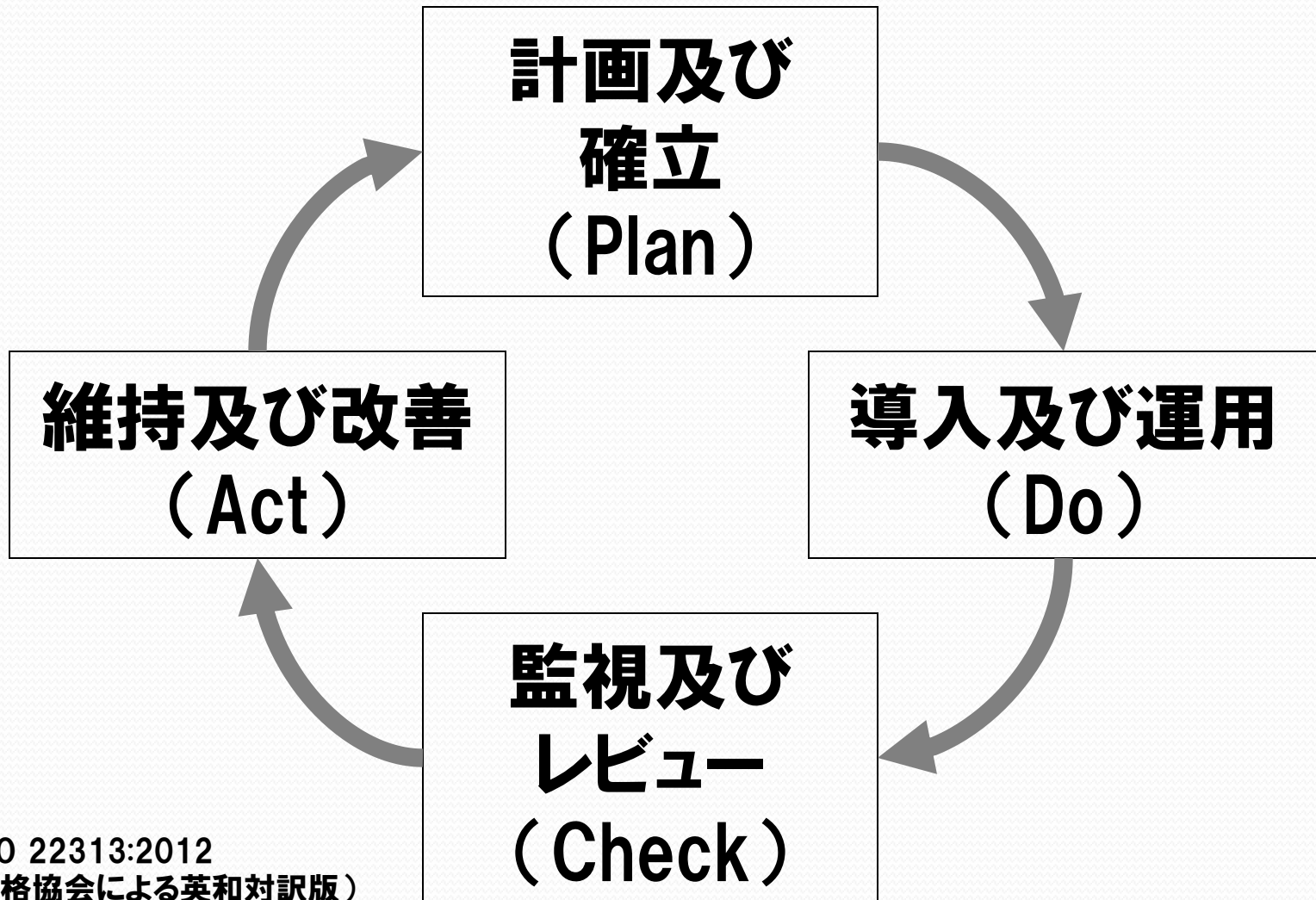
BCMSに関する世界共通言語として通用する

# BCMライフサイクル



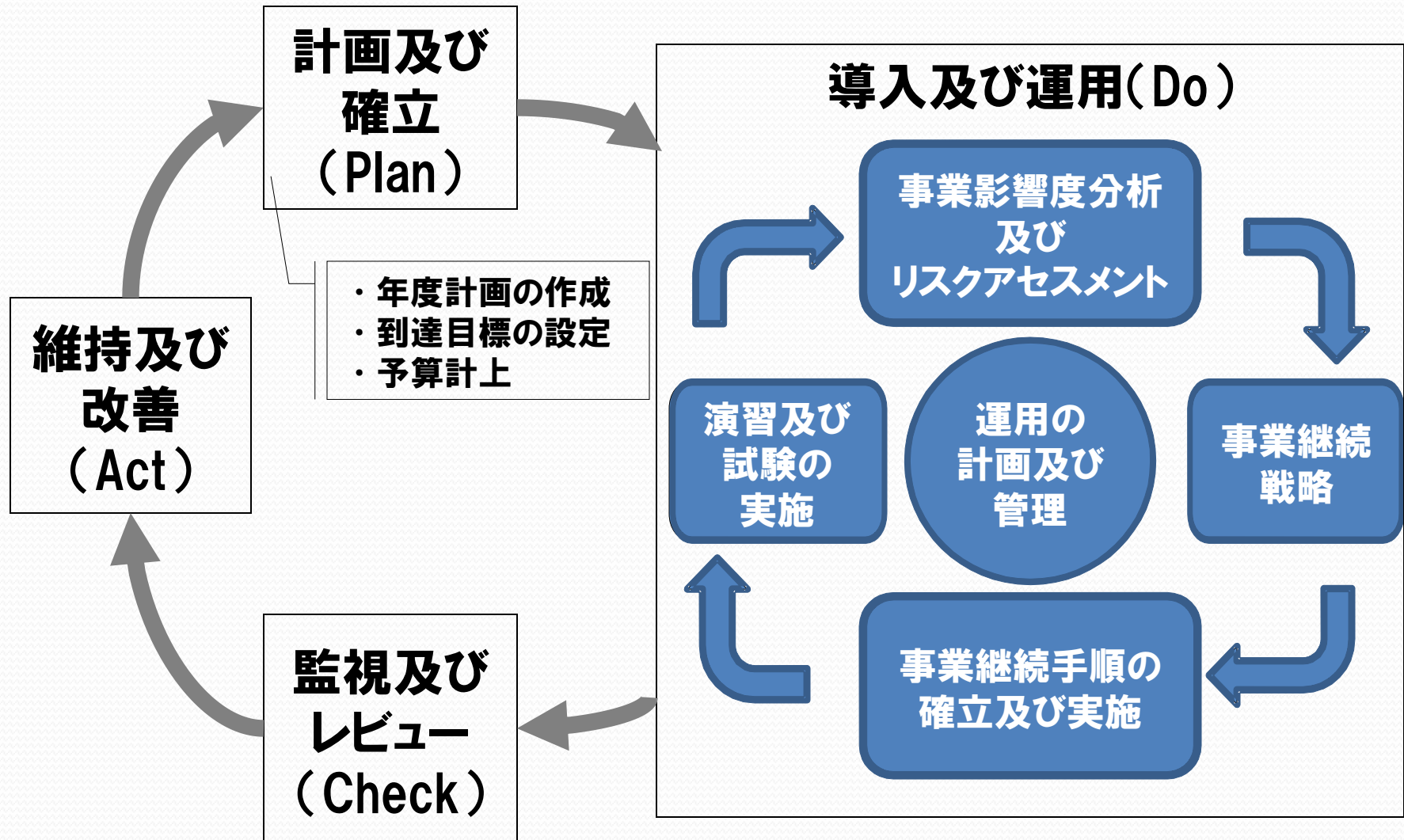
参考:ISO 22313:2012(日本規格協会による英和对訳版)

# 一般的なPDCAサイクル



参考:ISO 22313:2012  
(日本規格協会による英和対訳版)

# 事業継続マネジメントシステム

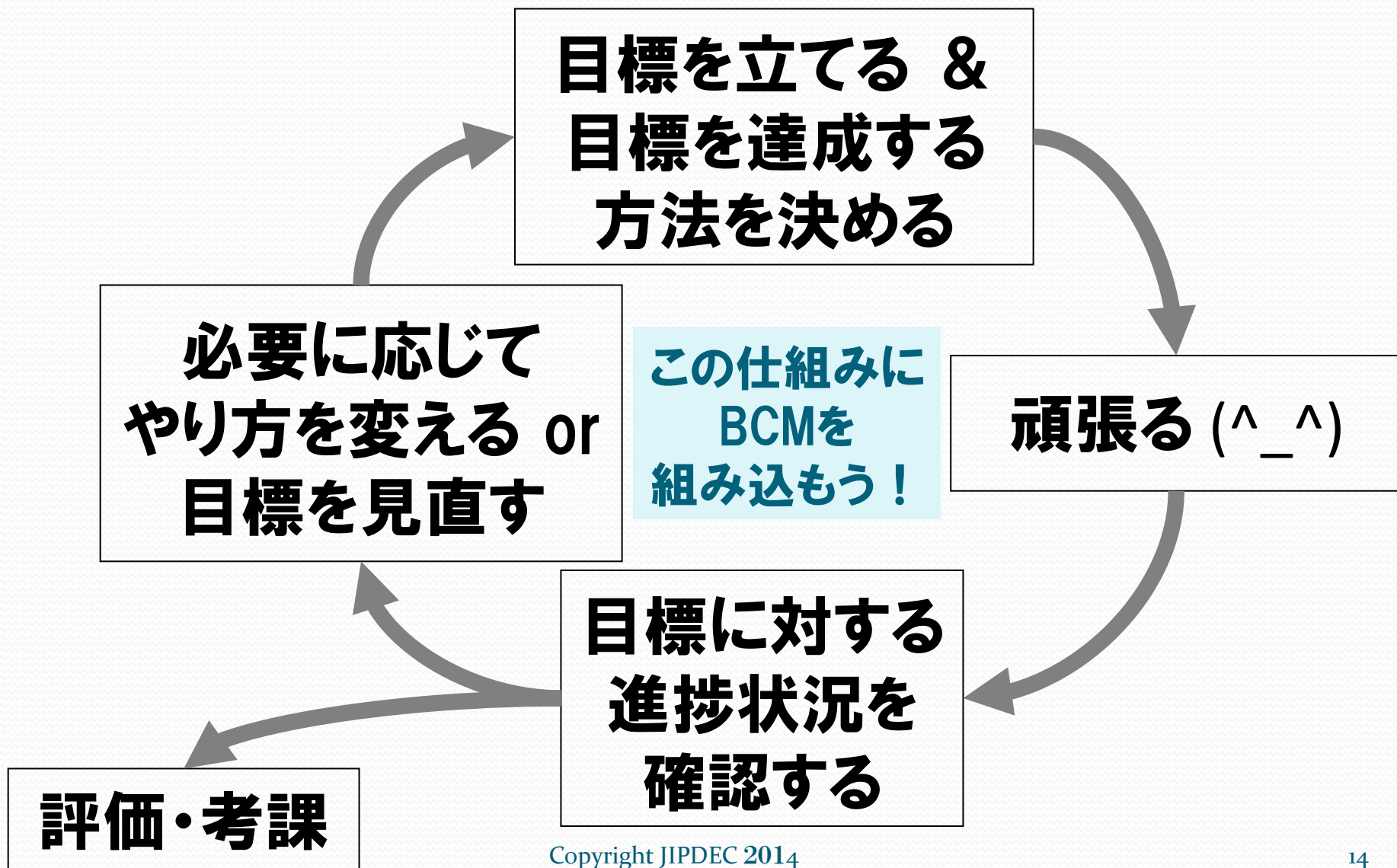


参考:ISO 22313:2012(日本規格協会による英和对訳版)

## 6. 計画

- ISO MSS共通要素における「計画」には、「マネジメントシステム全体についての計画」と「マネジメントシステムの意図する結果を実現するための計画」との2つの計画がある。
- 6章は、マネジメントシステム全体についての計画
  - BCMSそのものを定める「4. 4 事業継続マネジメントシステム」を満たす全体計画として、マネジメントシステムを構成するプロセス群をシステムとして運用するための計画がどうあるべきかが定められている。
  - その具体策が、「6. 1 リスク及び機会に対応するための処置」と「6. 2 事業継続目的及び達成計画」になる。
- 「8.1 運用の計画及び管理」は、マネジメントシステムの意図する結果を実現するための計画

# よくあるマネジメントシステムの例



# BCMS における目標を設定する

- 目標復旧時間(RTO)とは限らない
- BCMSによって、どのような状態を実現したいかを考え、その実現度合いを表す目標を設定する。
- SMART な目標になっているか？
  - **S**pecific --- 具体的な
  - **M**easurable --- 測定(判定)可能な
  - **A**ction oriented --- 行動を伴う
  - **R**ealistic --- 現実的な(実現可能な)
  - **T**ime sensitive --- 時間的制約のある



パフォーマンス  
指標

(参考: NFPA1600 2013 Edition)

## 9. パフォーマンス評価

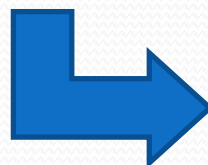
- (1) 概要
  - 以下のISO MSSでは次の3つを必須プロセスと定めている
    - 「監視、測定、分析及び評価」、「内部監査」、「マネジメントレビュー」
  - ISO 22301では、上記の3つに、**事業継続手順の評価(9. 1. 2)が追加され、4つの必須評価プロセス**となっている。事業継続手順の評価とは、演習と並んでBCM分野で広く行われてきた**“BCMの取組み”のレビューを、事業継続手順(8. 4)に特化した評価**として定められたもの。
- (2) 有効性
  - BCMSを運用した結果として、設定されていた目標が、どの程度達成できたのかがBCMSの有効性。
    - この有効性には効率の概念(達成された結果と、使用された資源との関係)は含まれていない(組織が自らの判断で効率の概念も含めるのは自由だが)。
  - 有効性の改善とは、目標が達成できるよう、さらにBCMSを改善することであり、例えば、BCMSを変更することによって、業務プロセスの阻害回数や利害関係者からの苦情など、組織が定めた不適合が減少することが有効性の改善にあたる。
  - ISO22301では、パフォーマンスを改善するために組織が設定する目標そのものを高めることは要求されていない点には注意が必要。(組織が自らの判断で要求するのは自由だが)
- (3) パフォーマンス
  - **パフォーマンスは「測定可能な結果」、パフォーマンス評価は「測定できる結果を確定するプロセス」という定義。**
  - 組織はBCMSのパフォーマンスの定義やそれを評価する指標、組織のニーズに適したパフォーマンスの測定基準を自ら設定の必要有。→今後実績を積んでガイド等出せば良いと考える。

# パフォーマンス指標を決める

- 「わが社はBCMSに取り組むことによって、どのような状態を実現したいのか？」
  - 自社がどのような状況に置かれているか、関係者間での共通理解が必要
  - トップマネジメントを含めてこのような議論を行い、社内でコンセンサスを得る



- それらがどのくらい実現できたかを表すものは何か？



**パフォーマンス指標**

## 4. 1 組織とその状況の理解 (1)

- (1) 組織内外の事項の決定と、それらを考慮してPDCAを回す

組織は、その目的に関係し、BCMSの**意図する結果**を達成する能力に影響する組織内外の事項を決定しなければならない。

組織のBCMSを確立し、導入し、維持するにあたって、これらの事項が考慮されなければならない。  
(ISO 22301:2012 4.1より)

- 組織が目指す「意図する結果」を達成する能力に影響する外部の状況(価値観に影響を与える社会の文化や経済環境等や組織の経営に直接影響を与える環境の変化等)や内部の状況(組織の製品・サービス、活動、資源、組織内利害関係者、組織構造等)の事項が何かを明らかにすることを求めている。
- ISO 22301の「意図する結果」は、箇条1の適用範囲から、その組織における重要な業務について、「**業務の阻害・中断を引き起こすインシデントを予防し、その起こりやすさを低減し、発生に備え、発生した場合には対応し、事業を復旧する**」ことである。

## 4. 1 組織とその状況の理解 (2)

- (2) 事業環境、組織の目的及び他の方針との関連、リスク選好の特定と文書化

組織は、次の事項を特定し、文書化しなければならない。

- a) 組織の活動、機能、サービス、製品、取引関係、サプライチェーン、利害関係者との関係、及び業務の中断・阻害を引き起こすインシデントに関係する潜在的な影響
- b) 事業継続方針と総合的なリスクマネジメント戦略を含む組織の目的及び他の方針との関連
- c) 組織のリスク選好

(ISO 22301:2012 4.1より)

- a) では事業環境として次の特定と文書化を求めている。
  - **事業の構成要素**：組織の提供しているサービス・製品とそれを支える組織の活動及び機能が何かを特定し文書化する。適用範囲を決める前の分析であるので、組織全体のサービス・製品、活動、機能をあまり細かくなりすぎず、適用範囲を決めるに十分な程度の分類で特定し文書をするが良い。
  - **連携関係**：組織を取り巻く顧客との取引関係、サプライヤとの取引関係、サプライチェーン、利害関係者との関係を特定し文書化する。
  - **事業中断が与える影響**：業務の中断・阻害を引き起こすインシデントによってどのような潜在的な影響が起こりうるかを特定し文書化する。
- b) では組織の目的及び他の方針との関連を文書化することを求めている。
  - 組織の目的に事業継続方針や他の方針がどう関わっているかなどを文書化
- c) ではリスク選好の明確化と文書化を求めている。
  - 次頁

# リスク選好

## リスク選好

組織に追及する又は保有する意思があるリスクの量及び種類

- リスク選好は、組織が意思を持って、組織全体としてどの程度のリスクをとるのか(保有するのか)、あるいはとらないのかについて、そのリスクの量や種類を示すことをいう。
- 重要な点は、リスクと戦略が常に絡み合わされていること
- リスク選好の管理
  - 策定(develop)／修正(revise)→コミュニケーション(communicate)→モニタリング(monitor)というサイクルで管理
  - リスクも組織の目的も、時が経つにつれ変容するため、一度策定されたリスク選好をそのまま放置せず、上記のようなサイクルで管理することが重要
- リスク選好の可視化、文書化が必須
  - 上記のリスク選好の管理サイクルを動かすためには、リスク選好の可視化、即ち文書化が必須となる
- ベンチャービジネスと社会インフラ業種
  - ベンチャービジネスと電力・通信・交通機関等の社会インフラ業種では、リスク選好が大きく異なる場合がある。積極的にリスクをとっていくのか、極力リスクを避けるのか、その程度を組織の置かれた状況から考慮

## 4. 2 利害関係者のニーズ及び期待の理解

### ● 4. 2. 1 一般

- BCMSに関連のある利害関係者の特定と、これら利害関係者の要求事項が何であるのかを決定することが求められている。
- 利害関係者としては、顧客、株主、債権者、会社のオーナー、従業員、従業員の家族、地域住民、業務委託先、仕入先、規制当局、競合他社、圧力団体、メディア、緊急サービス(警察や消防)等がある

### ● 4. 2. 2 法令及び規制の要求事項

- (1)事業継続に関連する法令及び規制の要求事項を文書化する
  - 事業継続に係る法令や規制として消防法や災害対策基本法や個人情報保護法等を明らかにするのみでなく、その要求事項を明らかにすることが必要。例えば、個人情報保護法は安否確認のために連絡先を入手することに関係するが、文書化する際には、単に「個人情報保護法」と記載するのみでなく、「利用目的を通知して入手」といった要件を明らかにしておく必要がある。
- (2)最新版の反映と周知方法の明確化
  - 法令規制の変更状況をチェックし、事業継続に関するものは最新化しておく必要がある。また、変更内容に対して影響を受ける従業員や利害関係者に周知しなければならない。
- (3)法令や規制の順守の確認の明確化
  - 組織によっては内部監査で確認しているところもある

# パフォーマンス指標の例

- 「顧客の安心感を高めたい」
  - --> 顧客からのアンケートや問合せへの回答状況
  - --> 顧客からのフィードバック
- 「有事の際に自発的に行動できる組織にしたい」
  - --> 意識向上プログラムの実施状況
  - --> 上記プログラム参加者からのフィードバック
- 「原材料の供給途絶のリスクを小さくしたい」
  - --> サプライヤのリスクアセスメントの進捗状況
- 「全ての BCP が検証済みの状態を常に維持したい」
  - --> 演習による BCP のカバー範囲
- 「BCM にかかるコストを少なくしたい」
  - --> BCM 関連予算／実績



**トップマネジメントを含む  
全ての関係者が納得できる  
パフォーマンス指標を  
設定することが  
経営課題として組織的に  
BCMに取り組むことに繋がる**

# パフォーマンス評価の方法

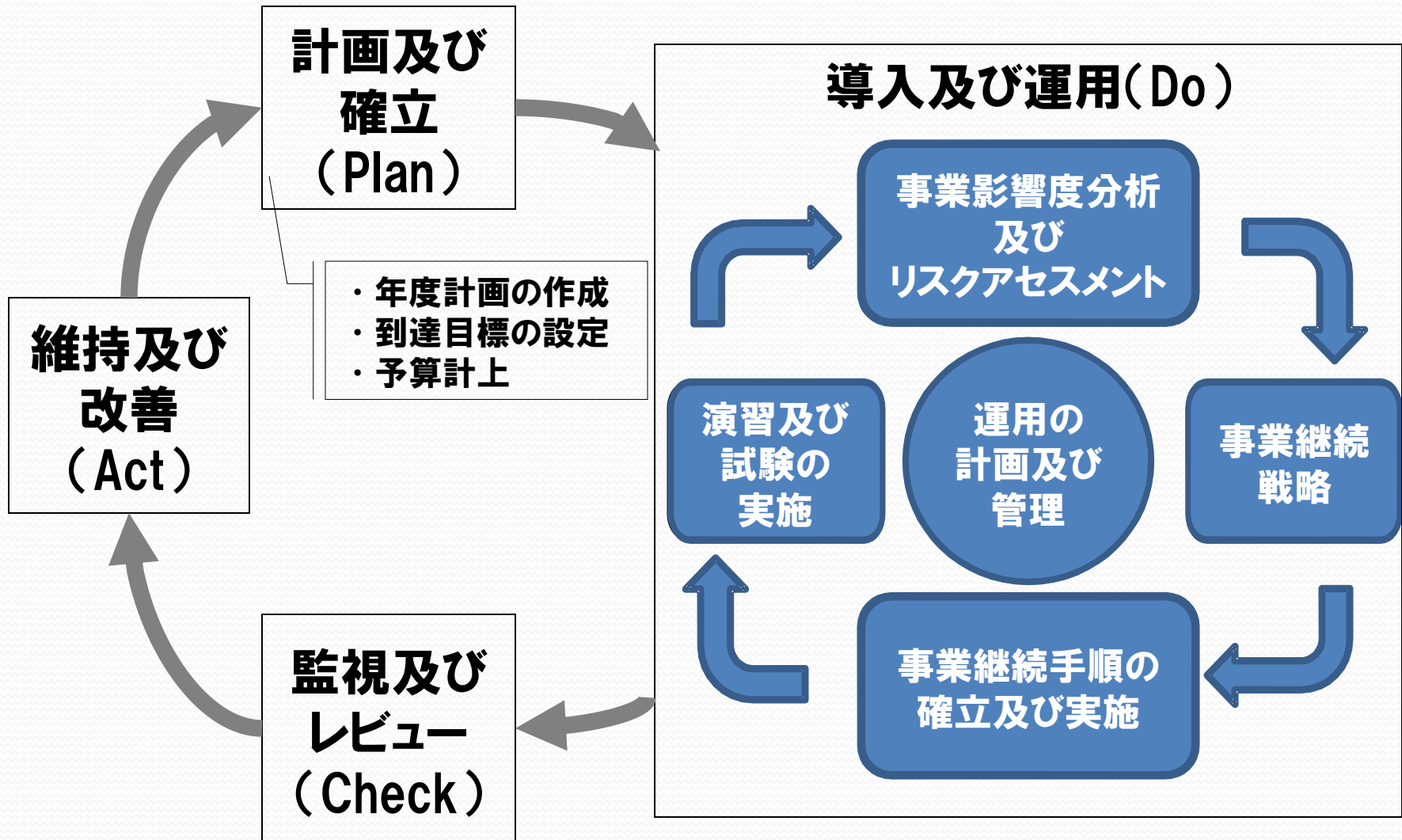
- 監視、測定、分析及び評価
  - 監視 (monitoring) には検査や試験を含む
  - 事業継続手順の評価
    - 定期的なレビュー、演習、試験、インシデント発生後の報告等
    - 法令及び規制の要求事項の遵守、業界のベストプラクティスとの適合、組織の事業継続方針及び目的との適合を定期的に評価
- 内部監査
- マネジメントレビュー



## よくある質問

**「うちの会社の BCM は  
どこまでやれば  
いいんでしょうか？」**

# 事業継続マネジメントシステム



参考:ISO 22313:2012(日本規格協会による英和对訳版)



**「うちの会社の BCM は  
どこまでやれば  
いいんでしょうか？」**



**BCMS に取り組む中で  
必要なレベルを自ら見出す**

BCP を策定するだけなら、  
担当者レベルでも(とりあえず)出来る。

BCM ライフサイクルを回すだけなら、  
担当部門に任せておいても(ある程度)出来る。

➡ 組織のレジリエンスも、それなりに高まる

経営層が、  
自組織に必要なレベルのレジリエンス向上を  
本気で目指そうと思ったら、  
必然的に BCMS という形で取り組むことになる。

# ご清聴ありがとうございました。

「BCMSユーザーズガイド」および  
BCMS適合性評価制度に関するお問い合わせ先

JIPDEC 情報マネジメント推進センター

<http://www.isms.jipdec.or.jp>



Copyright JIPDEC 2014