2009年11月
BCMSの認証制度と認証基準

BSIジャパン
教育事業部　事業部長
打川和男

raising standards worldwide™

講演者紹介

打川和男（うちかわ　かずお）

所属：BSIジャパン（英国規格協会）	教育事業部　事業部長

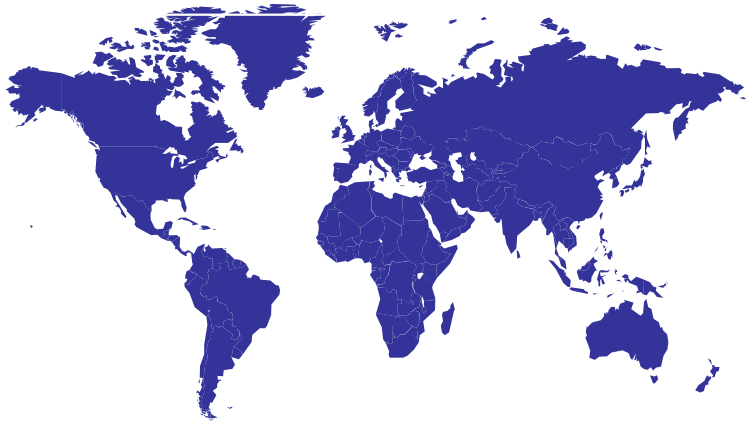
JIPDEC(日本情報処理開発協会) BCMS適合性評価委制度　実証運用技術部会　委員

JRCA登録　品質マネジメントシステム審査員(ISO9001)
CERA登録　環境マネジメントシステム審査員(ISO14001)
JRCA登録　情報セキュリティマネジメントシステム審査員(ISO/IEC27001)
IRCA登録　ITマネジメントシステム審査員 (ISO/IEC20000)
IRCA登録　労働安全衛生マネジメントシステム審査員(OHSAS18001)

編著：図解入門ビジネス　最新ITL V3の基本と仕組みがよ～く分かる本（秀和システム社）
編著：図解入門ビジネス　地球温暖化の基本と仕組みがよ～く分かる本（秀和システム社）
編著：図解入門ビジネス　事業継続管理の基本と仕組みがよ～く分かる本（秀和システム社）
編著：図解入門ビジネス　IT統制がよ～く分かる本（秀和システム社）
編著：図解入門ビジネス　ISO20000がよ～く分かる本（秀和システム社）
編著：図解入門ビジネス　ITILがよ～くわかる本（秀和システム社）
編著：図解入門ビジネス　最速プライバシーマーク取得がよ～くわかる本　新JIS対応版（秀和システム社）
編著：「市場の失敗事例に学ぶ」情報セキュリティポリシーの実践的構築手法（オーム社）
共著：個人情報保護法と企業対応（清分社）

BSIの紹介

- 英国の貿易産業省の支援を受けて設立された　世界最古の国家規格協会（1901年）
- 英国及びヨーロッパの標準化促進のため多種の規格開発
- 英国王室より英国王室憲章（Royal Charter)を授与（1929年）
- 1999年；BSIジャパン株式会社設立は1999年
- 現在、100カ国以上の国々で2,000人のスタッフが活動中



BSI グループ

BSI British Standards
英国国家規格開発及び発行

BSI Management Systems
- マネジメントシステムに関する審査及び認証登録サービスを提供100カ国以上、60,000件を超える認証登録
- 各国BSIで標準化されたトレーニングサービスを提供

BSI Product Services
製品認証及び検査サービスを提供

BSIの紹介

- BSIが開発、発行した主要なマネジメント規格

1979 **BS 5750** - ISO 9001（規格原案） 品質マネジメント
1992 **BS 7750** - ISO 14001（規格原案） 環境マネジメント
1995 **BS 7799** - ISO/IEC 27001（規格原案） 情報セキュリティマネジメント
1996 **BS 8800** - OHSAS 18001 労働安全衛生マネジメント
1999 **BS 8900** - *ISO26000 (規格原案の一部） 社会的責任マネジメント(SR)*
2000 **BS 8600** - ISO10002 (規格原案の一部） 苦情マネジメント
2002 **BS15000** - ISO/IEC20000 (規格原案) ITサービスマネジメント
2003 **PAS 56** - 事業継続マネジメント（ガイド）
2006 **PAS 99** - 統合マネジメント
2006 **BS25999-1** - ISO22399 (規格原案の一部) 事業継続マネジメント（ガイド）
2007 **BS25999-2** - ISO22301 (規格原案の一部) 事業継続マネジメント（仕様）
2007 **PAS77** - IT継続マネジメント（ガイド）
2008 **BS8901** - サスティナブルイベントマネジメント
2008 **BS31100** - *ISO31000 (規格原案の一部)*
2008 **BS25777** - IT継続マネジメント（ガイド）
2009 **BS16001** - *ISO50001 (規格原案の一部) エナジーマネジメント*

Contents

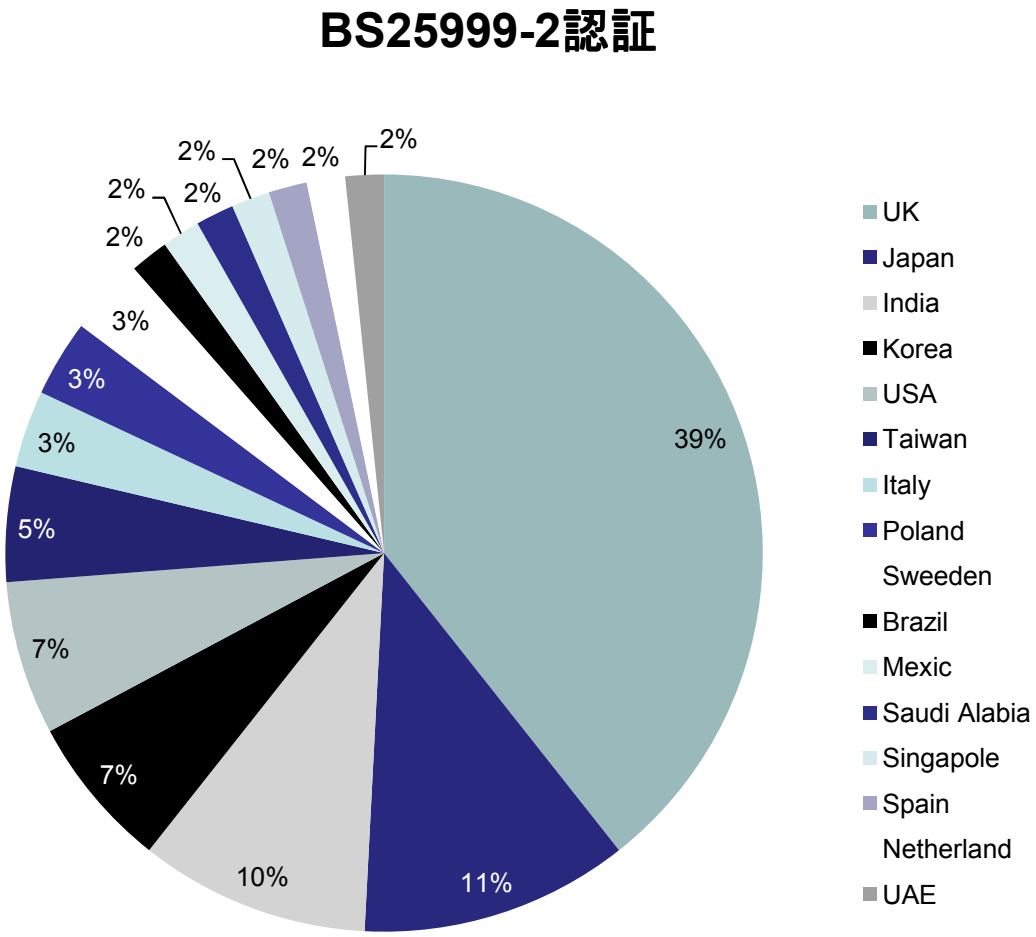
- 事業継続に関する第三者認証制度の動向
  - 各国のBCMに関する第三者認証制度
  - 各国のBSIが認証したBS25999-2の認証件数(UKAS)
  - 日本のBSIが認証したBS25999-2の組織
- BCMSに関するグローバルスタンダードBS25999-2の認証基準
- 事業（業務）継続に関する国際規格
  - ISO/TC223の状況
  - ISO22301 CDとBS25999-2:2007の比較
  - ISO22301のISO化の進捗状況

事業継続に関する第三者認証制度の動向

各国のBCMに関する第三者認証制度の動向

- 英国
  - UKASが2008年4月よりBS25999-2認定制度を開始
    - 現在、BSIを含む2機関が認定を受け、認証業務を実施中
- 日本
  - JIPDECがBCMS適合性評価制度を2010年4月より開始予定
    - 認証基準はBS25999-2:2007
- 米国
  - 任意認証制度を策定中
    - 組織のレジリエンスに係るマネジメントシステム規格を2009年3月にASISが、BSIの連携とともに発行

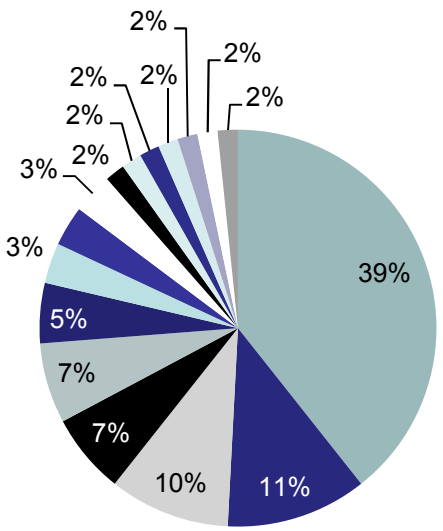
各国のBSIが認証したBS25999-2の認証件数(UKAS)



UK	24
Japan	7
India	6
Korea	4
USA	4
Taiwan	3
Italy	2
Poland	2
Sweden	2
Brazil	1
Mexico	1
Saudi Arabia	1
Singapore	1
Spain	1
Netherland	1
UAE	1
	61

日本のBSIがBS25999-2を認証した組織

BS25999-2認証



- UK
- Japan
- India
- Korea
- USA
- Taiwan
- Italy
- Poland
- Sweeden
- Brazil
- Mexic
- Saudi Alabia
- Singapole
- Spain
- Netherland
- UAE

- 富士通グループ
- コクヨファーニチャー
- 企業年金連合会
- クリエイトラボ
- NTTデータポップ
- NEC
- 日本興亜損保


Certificate of Registration

事業継続マネジメントシステム

企業年金連合会
〒105-0011
東京都
港区
芝公園2-4-1
芝パークビル8館10階

Pension Fund Association
2-4-1 Shiba-koen,
Minato-ku,
Tokyo
105-0011
Japan

上記組織は認証登録範囲に記述された活動について

BS 25999-2:2007

の要求事項に適合した

事業継続マネジメントシステムを実施しています。

認証登録番号: BCMS 537752

For and on behalf of BSI:

代表取締役 徳永 光正

初回認証登録日: 2008/11/12

BSI Management Systems

BCMSに関するグローバルスタンダード
BS25999-2の認証基準

raising standards worldwide™

BS25999の概要

- 事業継続マネジメントの英国国家規格
- **BS25999-1:2006とBS25999-2:2007の二つの規格からなる**
  - BS25999-1:2006 事業継続マネジメントのための実践規範（Code of practice）–2006年11月発行
  - BS25999-2:2007 事業継続マネジメントのための要求事項(Specification) –2007年11月発行

BS25999-2:2007の認証基準

3 事業継続マネジメント システムの計画	3.1 概要
	3.2 BCMS の確立及び管理
	3.3 組織の文化にBCM を組み込む
	3.4 BCMS の文書及び記録
4 BCMS の導入及び運用	4.1 組織の理解
	4.2 事業継続戦略の決定
	4.3 BCM 対応の開発及び導入
	4.4 BCM の取組みの演習，維持及びレビュー
5 BCMS の監視及びレビュー	5.1 内部監査
	5.2 BCMS のマネジメントレビュー
6 BCMS の維持及び改善	6.1 予防処置及び是正処置
	6.2 継続的改善

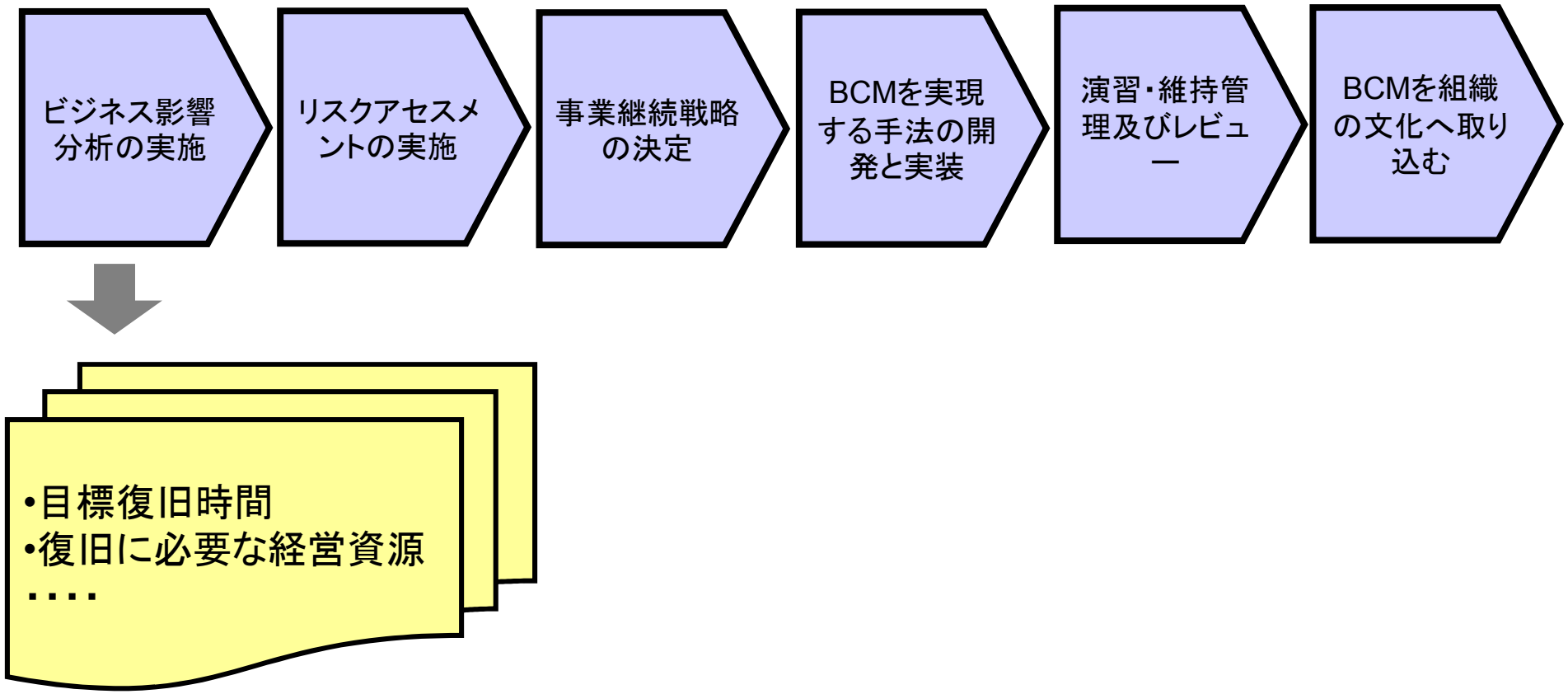
組織の理解(1/2)

キーワード:

◆事業インパクト分析

- ◆ 主要な製品及びサービスをサポートする活動の特定
- ◆これらの活動の中断(混乱)によって生じる影響の特定
- ◆最大許容停止時間の特定
- ◆重要な活動の特定(復旧の優先順位に応じた)
- ◆重要な活動に関連する依存関係の特定
- ◆供給者及び外部委託先(重要な活動が依存している)についてのBCM活動の取組みの明確化
- ◆目標復旧時間の設定
- ◆各重要な活動の再開に必要な経営資源の評価

組織の理解(1/2)


ビジネス影響分析の実施
リスクアセスメントの実施
事業継続戦略の決定
BCMを実現する手法の開発と実装
演習・維持管理及びレビュー
BCMを組織の文化へ取り込む
•目標復旧時間
•復旧に必要な経営資源
・・・・

組織の理解(2/2)

キーワード:

◆リスクアセスメント

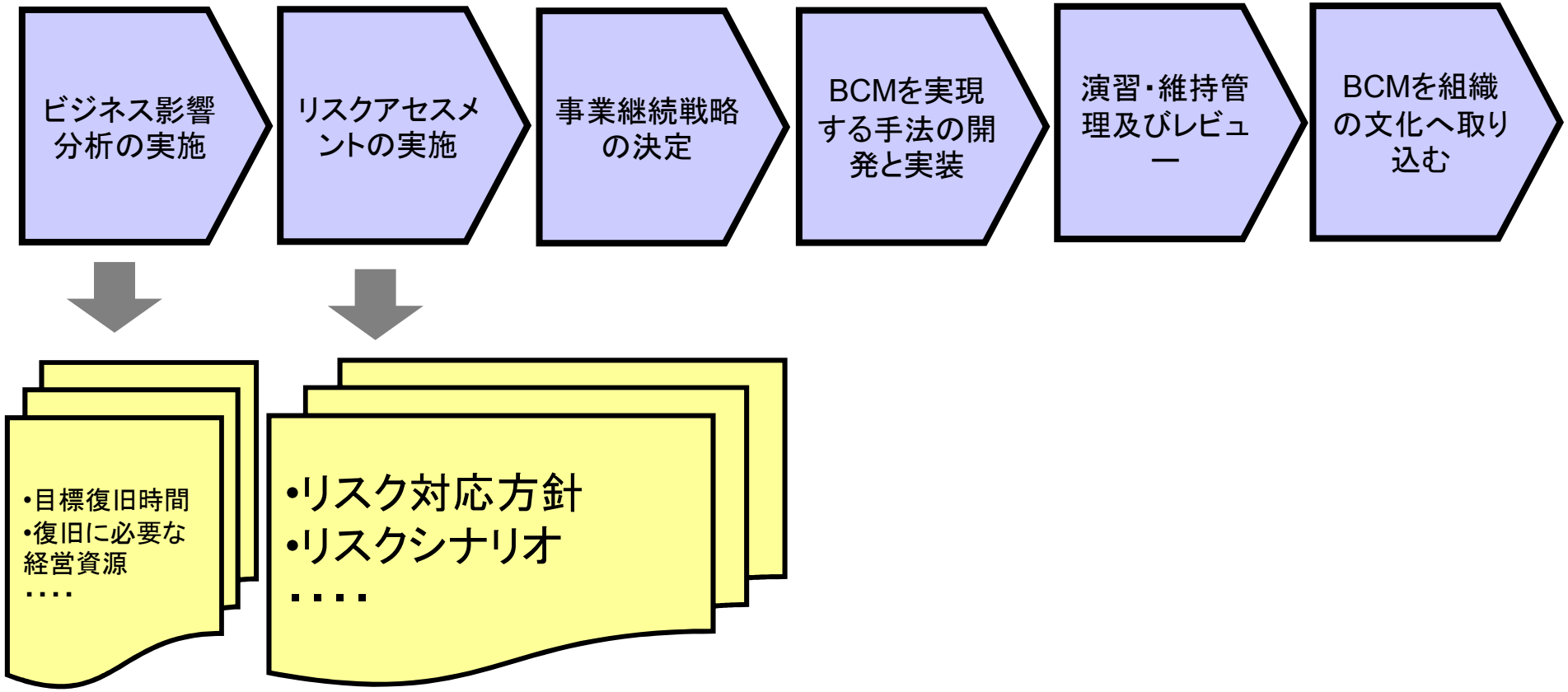
- ◆重要な活動と経営資源に対する脅威及びぜい弱性の理解
- ◆特定された脅威がインシデントになり，事業中断（混乱）をもたらした場合に発生する影響の理解

◆選択枝の決定

- ◆ 中断（混乱）の発生確率の低減
- ◆中断（混乱）の時間の短縮
- ◆主要な製品及びサービスに対する中断（混乱）の影響の限定

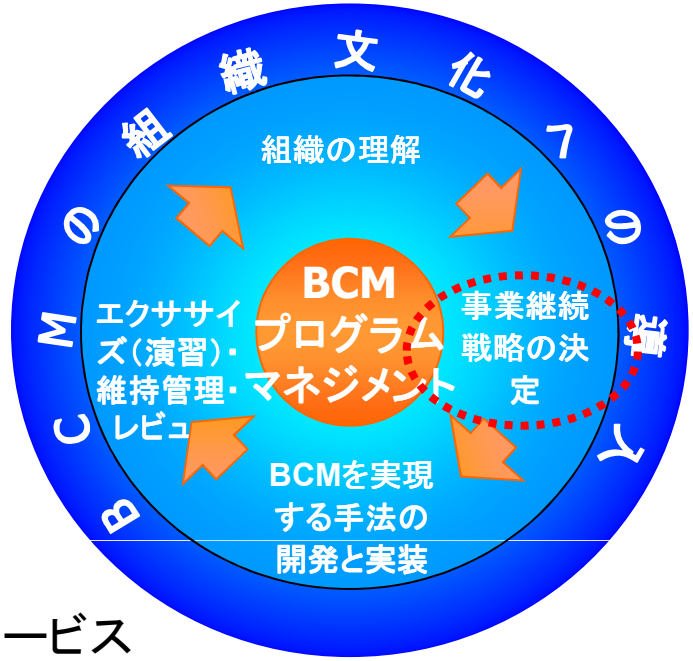
◆リスク対応策の決定

組織の理解(2/2)


ビジネス影響分析の実施
リスクアセスメントの実施
事業継続戦略の決定
BCMを実現する手法の開発と実装
演習・維持管理及びレビュー
BCMを組織の文化へ取り込む
•目標復旧時間
•復旧に必要な経営資源
・・・・
•リスク対応方針
•リスクシナリオ
・・・・

事業継続戦略の決定

キーワード:



◆中断(混乱)への対応と復旧のための体制の
　明確化(インシデントマネジメント体制)

◆BCMの取り組みの決定

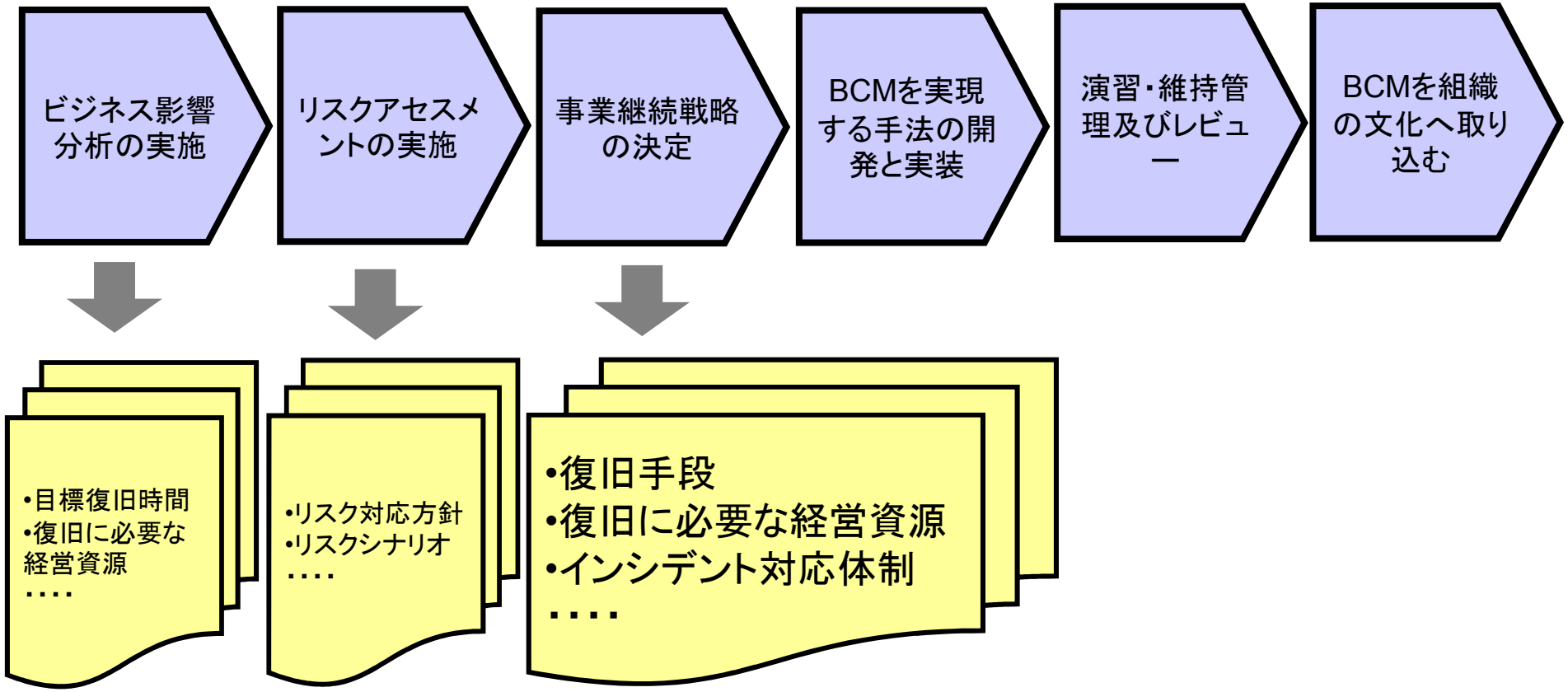
　◆重要な活動の復旧手段

　◆再開に必要な経営資源

　◆供給者及び外部委託先から供給される製品及びサービス

◆復旧に関連する主要なステークホルダー及び外部の関係者との関係管理手法の決定

事業継続戦略の決定

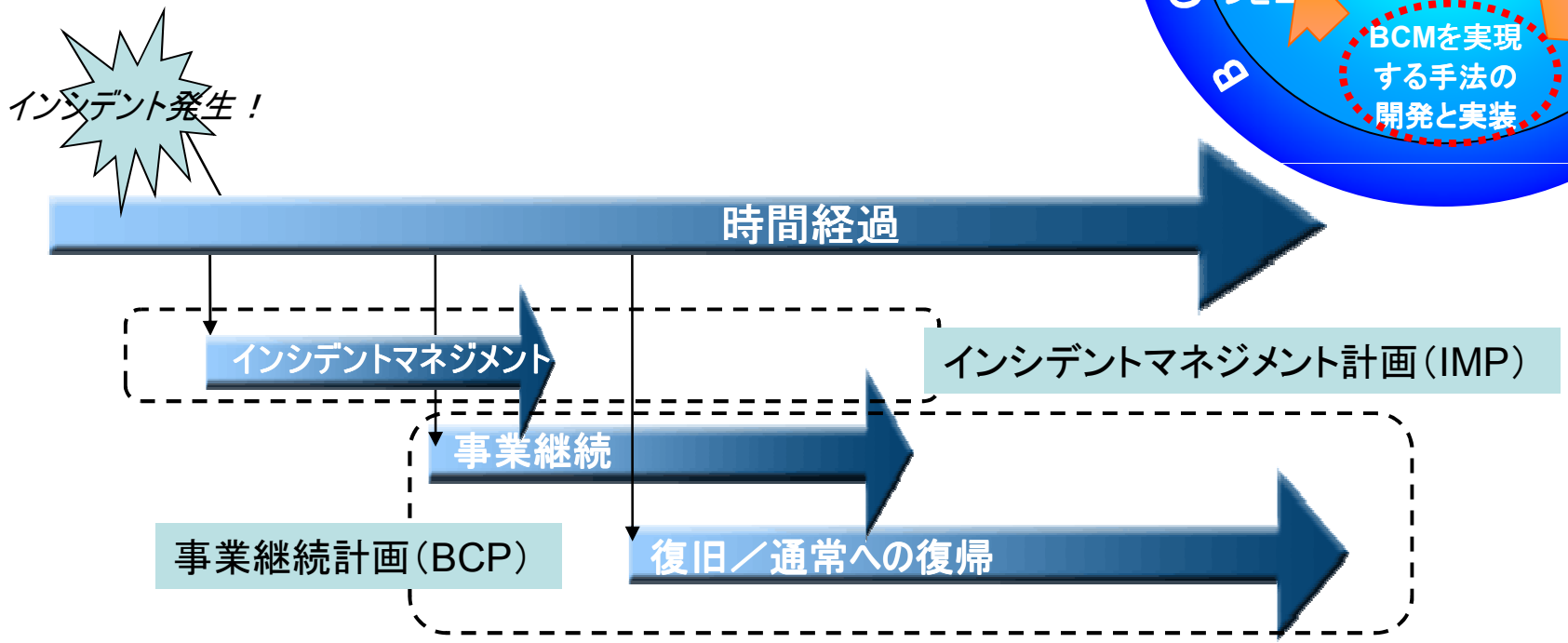

ビジネス影響分析の実施
リスクアセスメントの実施
事業継続戦略の決定
BCMを実現する手法の開発と実装
演習・維持管理及びレビュー
BCMを組織の文化へ取り込む
•目標復旧時間
•復旧に必要な経営資源
・・・・
•リスク対応方針
•リスクシナリオ
・・・・
•復旧手段
•復旧に必要な経営資源
•インシデント対応体制
・・・・

BCMを実現する手法の開発と実装

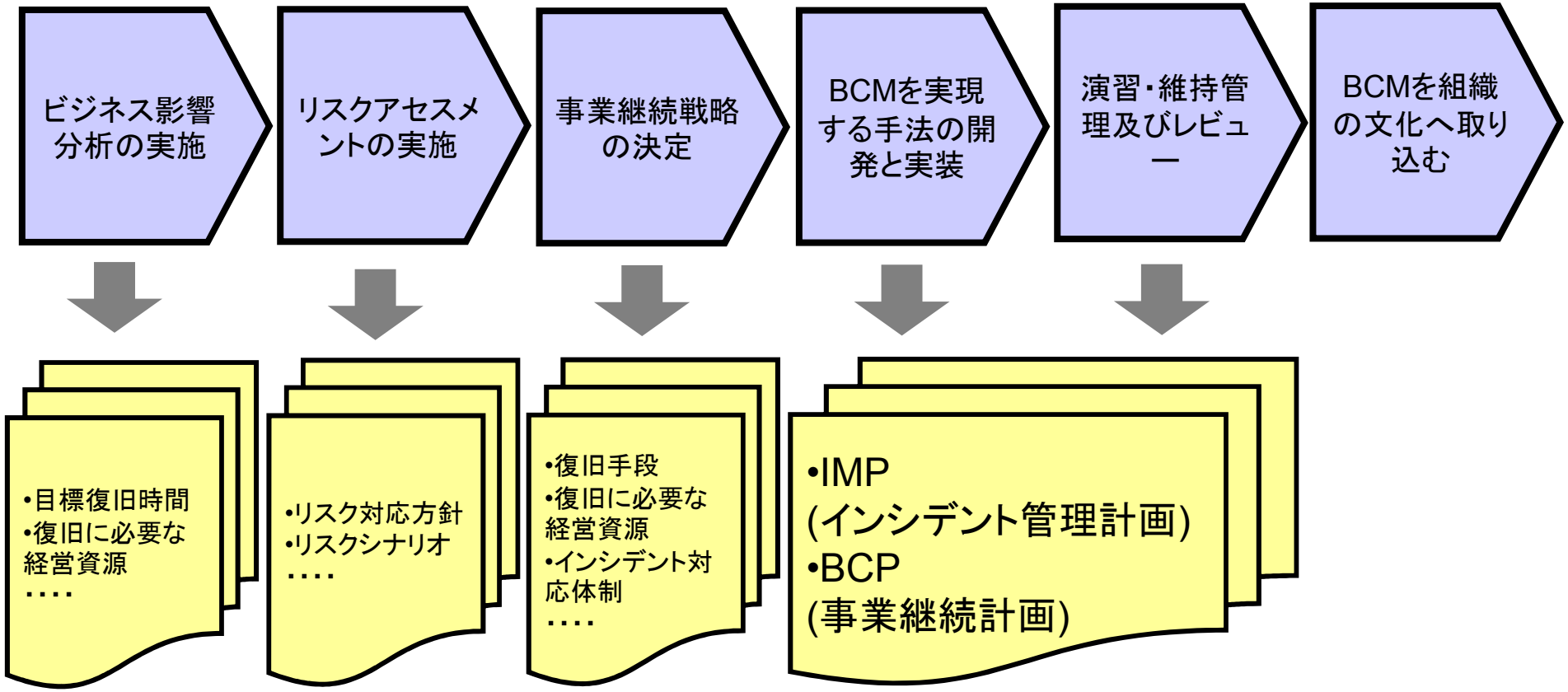
キーワード:

◆インシデントマネジメント計画の策定

◆事業継続計画の策定



BCMを実現する手法の開発と実装



演習・維持管理・レビュー

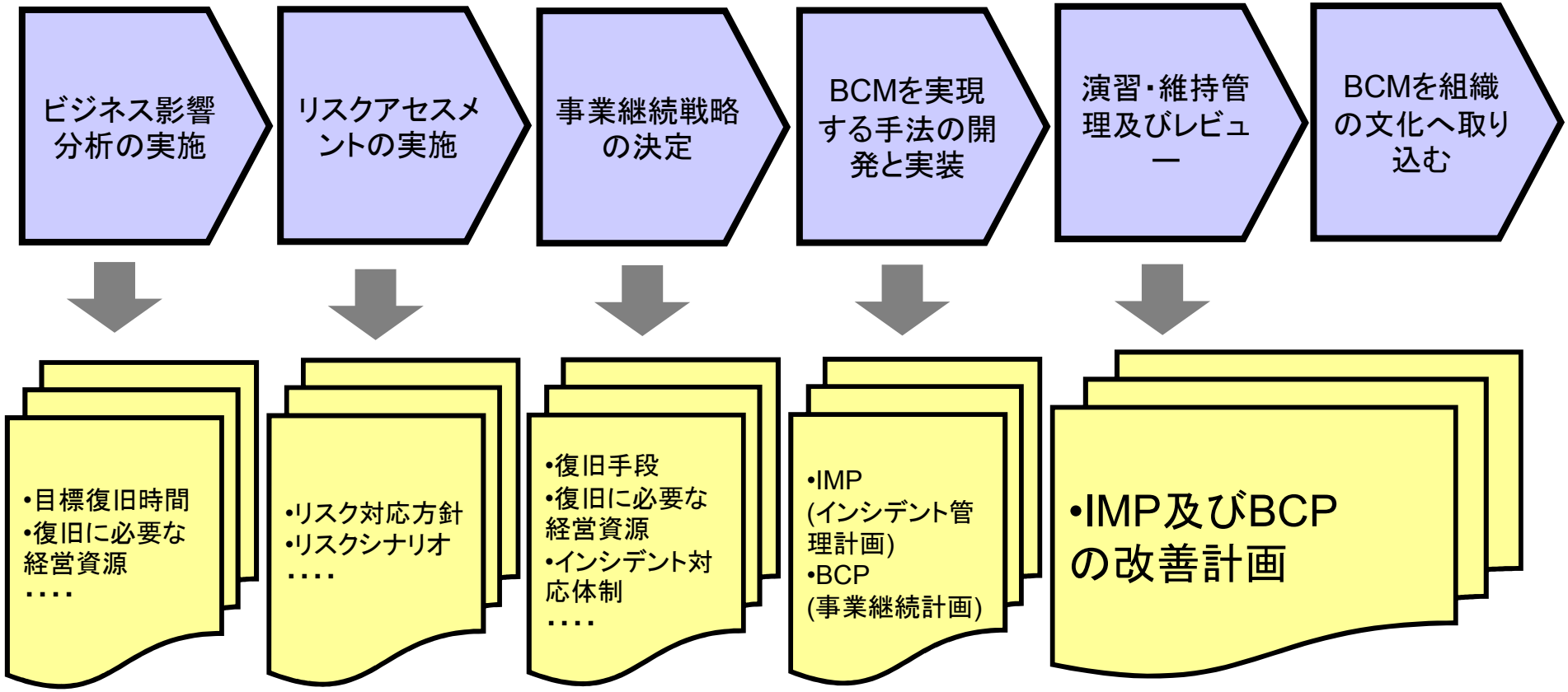
キーワード:

◆演習（エクササイズ）の実施
- ◆あらかじめ定めた間隔、重大な変更時に実施
- ◆演習を通じて妥当性を確認する
- ◆演習計画時には、演習によってインシデントが発生しないように考慮する
- ◆演習目的と目標を実施後に評価する

◆演習（エクササイズ）の手段（BS25999-1）
- ◆デスクトップレビュー
- ◆ウォークスルー
- ◆シュミレーション

◆BCM の取組みの維持及びレビュー
- ◆セルフアセスメント又は監査の実施
- ◆IMP、BCPの発動に至ったインシデント発生後のレビュー

演習・維持管理・レビュー


ビジネス影響分析の実施
リスクアセスメントの実施
事業継続戦略の決定
BCMを実現する手法の開発と実装
演習・維持管理及びレビュー
BCMを組織の文化へ取り込む
•目標復旧時間
•復旧に必要な経営資源
・・・・
•リスク対応方針
•リスクシナリオ
・・・・
•復旧手段
•復旧に必要な経営資源
•インシデント対応体制
・・・・
•IMP
(インシデント管理計画)
•BCP
(事業継続計画)
•IMP及びBCPの改善計画

BCMの組織文化への導入

キーワード:

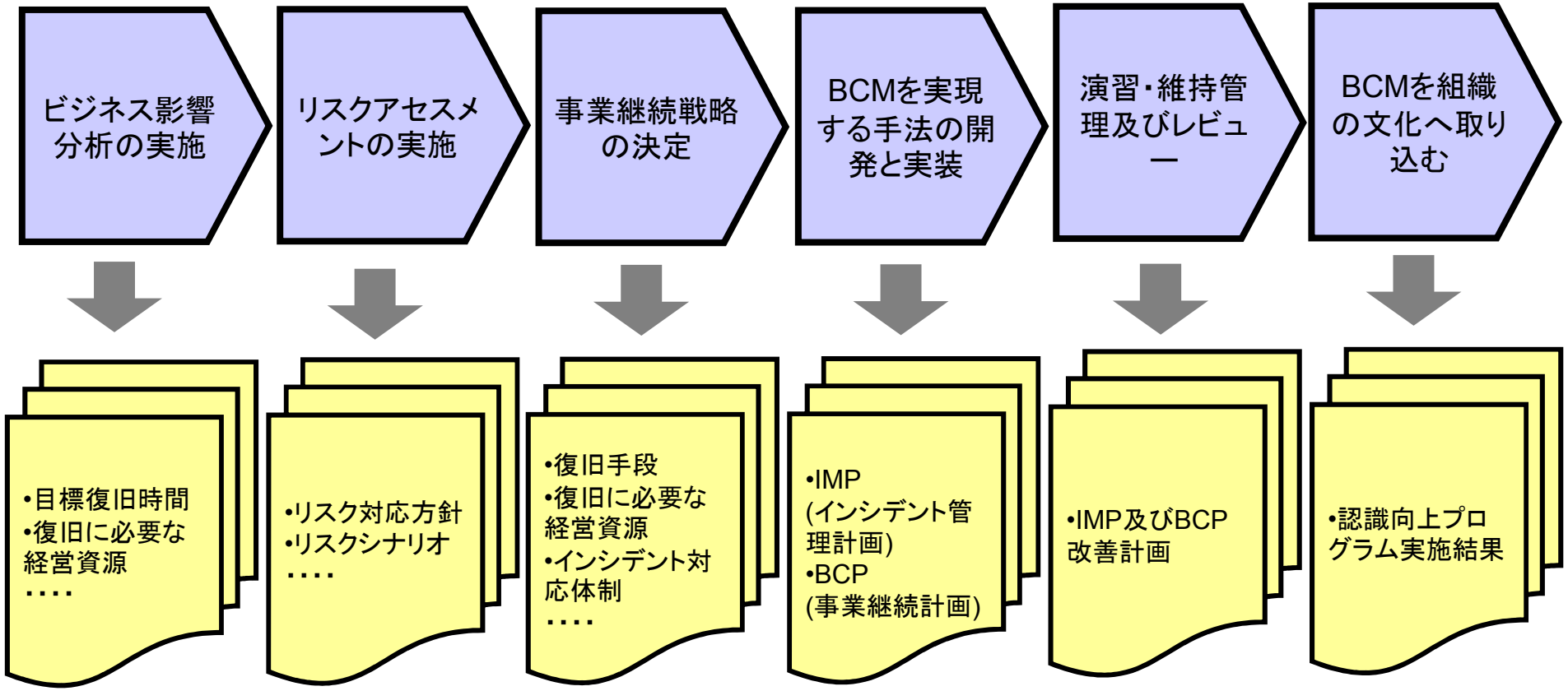
◆継続的なBCM教育の実施、認識向上プログラムの開発と実行、ならびに意識向上の有効性評価プロセスの確立

◆重要性の周知

- ◆事業継続マネジメントの目的に合致していること
- ◆事業継続方針に適合していること
- ◆継続的に改善すること

◆認識の向上（すべての従業員のBCMへの自己貢献）

BCMの組織文化への導入



事業（業務）継続に関する国際規格

ISO/TC223（社会的セキュリティ）の状況

- WG1: 主査日本
  - 社会セキュリティマネジメントの枠組み内部文章整備
    - ISO22397: 官民連携（提案準備）
    - ISO22398: 演習手順（提案準備）
- WG2: 主査英国
  - 社会セキュリティに関する用語規格集の提案
    - ISO22300(現在CDの投票中)・・・・ISO Guide 73と整合
- WG3: 主査ドイツ
  - 社会セキュリティにおける組織の指揮命令、協調に関する規格開発
    - ISO22320:緊急事態解決における指揮命令、及び協調のための原則
    - ISO22321:指揮命令及び協調・協力に関する情報要求事項
    - ISO22322:組織内外警報手順-緊急事態警報
- **WG4: 主査オランダ**
  - **緊急事態準備と業務継続に関する規格開発**
    - **ISO22399:ガイドライン**
    - **ISO22301:要求事項**

参考:

ISO Guide 73
リスクマネジメント – 用語
（現在、Draft段階）

ISO31000
リスクマネジメント – 原則及びガイドライン
（現在、FDIS段階）

※共にJIS化作業中

ISO22301 CDとBS25999-2:2007の比較

ISO22301 CD			BS25999-2:2007
4.2 経営者の責任	4.2.1 経営者のコミットメント		-
	4.2.2 方針表明		3 BCMSの計画 3.2.2 BCMの方針
	4.2.3 責任、権限及び伝達	4.2.3.1 責任及び権限	3 BCMSの計画 3.2.3 経営資源の提供 3.2.3.2
		4.2.3.2 管理責任者	3 BCMSの計画 3.2.3 経営資源の提供 3.2.3.3
4.3 PCMS要求事項	4.3.1 PCMSの適用範囲		3 BCMSの計画 3.2.1 BCMSの適用範囲及び目的
4.4 BIA及びリスクアセスメント			4 BCMSの導入及び運用 4.1 組織の理解
	4.4.1 法的及びその他の要求事項		-
	4.4.2 BIA		4 BCMSの導入及び運用 4.1.1 BIA
	4.4.3 リスクアセスメント		4 BCMSの導入及び運用 4.1.2 リスクアセスメント
4.5 文書化の要求事項	4.5.1 一般		3 BCMSの計画 3.4 BCMSの文書及び記録 3.4.1 概要
	4.5.2 文書の管理		3 BCMSの計画 3.4 BCMSの文書及び記録 3.4.3 BCMSの文書の管理
	4.5.3 記録の管理		3 BCMSの計画 3.4 BCMSの文書及び記録 3.4.2 BCMSの記録の管理
4.6 計画	4.6.1 目的及びその達成計画		-
	4.6.2 資源の提供		3 BCMSの計画 3.2.3 経営資源の提供 3.2.3.1

ISO22301 CDとBS25999-2:2007の比較

ISO22301 CD				BS25999-2:2007
5 PCMSの実施及び運用	5.1 リスク対応策の選択	5.1.1 リソースに関する要求事項の設定		4 BCMSの導入及び運用 4.2 事業継続戦略の決定
		5.1.2 保護及び軽減		4 BCMSの導入及び運用 4.1 組織の理解 4.1.3 選択の決定
	5.2 PCMSの力量及び認識	5.2.1 一般		3 BCMSの計画 3.2.4 BCM要員の力量
		5.2.2 力量		3 BCMSの計画 3.2.4 BCM要員の力量 3 BCMSの計画 3.3 組織の文化にBCMを組み込む
	5.3 緊急事態準備及び業務継続に関する要求事項	5.3.1 一般		4 BCMSの導入及び運用 4.3 BCM対応の開発及び導入 4.3.3 事業継続計画及びインシデントマネジメント計画 4.3.3.2
		5.3.2 保護及び軽減		-
		5.3.3 コミュニケーション及び警告		-
		5.3.4 緊急時対応		4 BCMSの導入及び運用 4.3 BCM対応の開発及び導入 4.3.2 インシデントマネジメント体制
			5.3.4.1 緊急事態対応手順に関する要求事項	4 BCMSの導入及び運用 4.3 BCM対応の開発及び導入 4.3.3 事業継続計画及びインシデントマネジメント計画 4.3.3.1
			5.3.4.2 緊急事態対応手順の内容	4 BCMSの導入及び運用 4.3 BCM対応の開発及び導入 4.3.3 事業継続計画及びインシデントマネジメント計画 4.3.3.3
		5.3.5 復旧		4 BCMSの導入及び運用 4.3 BCM対応の開発及び導入 4.3.3 事業継続計画及びインシデントマネジメント計画 4.3.3.3 o), p)
	5.4 緊急事態準備及び業務継続に関する訓練/テスト			4 BCMSの導入及び運用 4.4 BCMの取組みの演習、維持及びレビュー 4.4.2 BCMの演習

ISO22301 CDとBS25999-2:2007の比較

ISO22301 CD			BS25999-2:2007
6 PCMSの監視及びレビュー	6.1 パフォーマンス測定及び監視		-
	6.2 緊急事態準備及び業務継続に関する取り決めの評価		4 BCMSの導入及び運用 4.4 BCMの取り組みの演習、維持及びレビュー 4.4.3 BCMの取り組み維持及びレビュー
	6.3 PCMSの監査		5 BCMSの監視及びレビュー 5.1 内部監査
	6.4 経営者によるPCMSのレビュー		5 BCMSの監視及びレビュー 5.2 BCMSのマネジメントレビュー 5.2.1 概要
		6.4.1 経営者によるレビューのためのインプット	5 BCMSの監視及びレビュー 5.2 BCMSのマネジメントレビュー 5.2.2 レビューへのインプット
		6.4.2 経営者によるレビューからのアウトプット	5 BCMSの監視及びレビュー 5.2 BCMSのマネジメントレビュー 5.2.3 レビューからのアウトプット
7.1 継続的改善	7.1 継続的改善		6 BCMSの維持及び改善 6.1 予防処置及び是正処置 6.1.1 概要 6 BCMSの維持及び改善 6.2 継続的改善
	7.2 不適合、是正処置及び予防処置		6 BCMSの維持及び改善 6.1.3 是正処置 6 BCMSの維持及び改善 6.1.2 予防処置

ISO22301のISO化の進捗状況

- NWIP（国際規格提案）：済み　　ー提案段階

↓

- WD（作業原案）：済み　　ー作成段階

↓ 12ケ月

- CD（委員会原案）：済み　　ー委員会段階

↓ 6ケ月

- DIS（国際規格案）：　　ー照会段階

↓ 12ケ月

- FDIS（最終国際規格案）：　　ー承認段階

↓ 6ケ月

- IS（国際規格）：　　ー発行段階

2011年7月？

raising standards worldwide™

ご清聴ありがとうございました

Contact Us

Name: 打川和男　Kazuo Uchikawa
Title: 教育事業部　事業部長　Director, BSI Training -Japan
Email: kazuo.uchikawa@bsigroup.com