6.パフォーマンス評価による継続的改善
（上級者編）

個人情報保護・情報セキュリティをマネジメントする
監視・監査・是正・継続的改善

株式会社エム・ピー・オー
代表取締役 森口修逸

本日の内部監査員教育（上級編＋補講）の流れ

1. 内部監査員教育の基本の復習（e-learning初級者編より）
   - ✓ 「監査の定義」(8分間)
2. 今年の重要な出来事
   - ✓ 改正個人情報保護法復習
   - ✓ 医療・健診・産業保健分野におけるリスク
   - ✓ 安全管理に関する動向
   - ✓ 産業保健分野の重要な改訂
   - ✓ JISQ15001 :全体の復習
3. パフォーマンスを向上するために（上級編）
   - □ 8. 運用　8.1 現場管理者による運用確認の実務
   - □ 9. パフォーマンス評価　9.1 監視、測定、分析及び評価の実務
     - 9.2　追　内部監査の指摘のHowTo
   - □ 10. 改善　10.2 継続的改善のHowTo
     - 10.1　追　是正処置の改善力向上のHowTo
4. 今年の監査ポイント

内部監査員教育の基本の復習

- （e-learning初級者編より）
  - 「監査の定義」
    - ・ビデオ視聴（8分間）
- 今年度の重要な出来事
  - ✓ 改正個人情報保護法復習
  - ✓ 医療・健診・産業保健分野におけるリスク
  - ✓ 安全管理に関する動向
  - ✓ 産業保健分野の重要な改訂

✔ 改正個人情報保護法復習

改正個情法周辺の規範

概観

憲法　第13条　生命・自由及び幸福追求に対する国民の権利
第23条　学問の自由

労働安全衛生法等
医療法・医師法

優位

優位

個人情報保護法

・行政/独法個情法
・自治体条例

―個人情報保護委員会―
・政令・委員会規程
・個人情報保護ガイドライン
a.通則編、b.第三者提供編
c.匿名加工編,d.外国第三者編
・個人情報保護Q&A
・医療介護ガイダンス 、金融・通信

（厚労省）安全管理ガイドライン
（総務省）政令・規則・ガイドライン　等

次世代医療基盤法

「匿名化医療情報」

法の埒外　医学研究分野　厚労省・経産省・文科省

a.ゲノム研究GL、b.医学研究GL、c.遺伝子治療GL

医療機関・健診機関

- 個人情報
- 個人識別符号
- 要配慮個人情報
- 匿名加工情報
- 非個人情報　の識別

取得

利用提供

安全管理

開示

倫理委員会

「提供する」・「提供される」場合の記録

トレーサビリティの確保

法第二十五条
個人データを第三者に提供するとき

★記録事項
- 本人同意を得ている旨
- 第三者の氏名又は名称及び住所
- 本人の氏名その他、本人を特定できる事項
- 個人データの項目

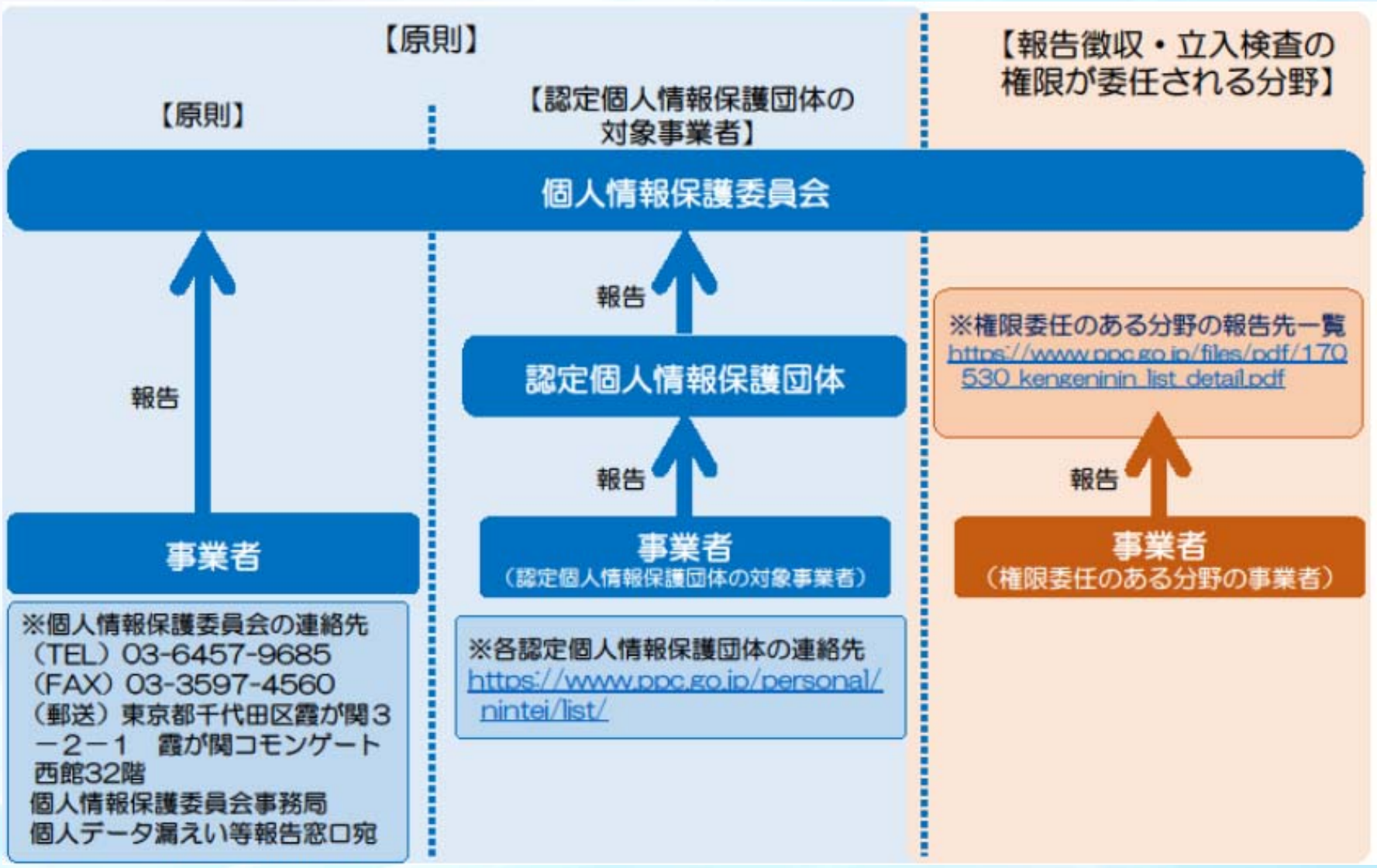
法第二十六条
第三者から個人データの提供をされたとき

★記録事項
- 本人同意を得ている旨
- 第三者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名
- 第三者による当該個人データの取得の経緯
- 本人の氏名その他、本人を特定できる事項
- 個人データの項目

記録の作成方法の別	保存期間
契約書等の方法で記録作成の場合	最後に提供を行った日から起算して1年を経過までの間
一括で記録を作成した場合	最後に提供を行った日から起算して3年を経過までの間
上記以外の場合	3年

★記録事項の省略可：複数回にわたり授受をする場合には重複記録の必要はない。

個人情報保護委員会への報告



改正個人情報保護ガイドライン

1. 通則編

個人情報保護法全体の解釈・事例を掲載し、全ての分野に共通に適用される汎用的なガイドラインで、各省のガイドラインは、これに一元化する。

a. 詳細な解説や事例等は本ガイドラインには記載せず、必要に応じてQ&Aやその他の解説資料等において記載。

b. 安全管理措置の内容は、原則、番号法ガイドライン[特定個人情報の適正な取扱いに関する ガイドライン(事業者編)]に準じる。

c. 医療関連、金融関連、情報通信関連　等については、上記ガイドラインを基礎として、 当該分野においてさらに必要となる別途の規律を定める。

d. 詳細な解説や事例等は必要に応じてQ&Aやその他の解説資料等において記載。

2. 外国にある第三者への個人データの提供編

法第24条に関する内容について、法及び 施行規則の基本的な解釈を記載。

3. 第三者提供時の確認・記録義務編

法第25条・第26条で定められる「個人データの第三者提供時における確認・記録義務」の内容について、法及び施行規則の基本的な解釈を記載。

4. 匿名加工情報編

匿名加工情報について、法及び施行規則の基本的な解釈を記載。

a. 適正な加工、 b. 安全管理措置、 c. 作成時・第三者提供時の義務、 d.識別行為の禁止

✔ 医療・健診・産業保健分野におけるリスク

ヘルスケア分野における監査とは

1. 個人情報保護に関するリスク
   - A) 不適切な取得、同意の獲得なし
   - B) 同上　利用、利用目的にない利用
   - C) 同上　提供、同意のない提供、法律外の提供
   - D) 同上　開示、開示の却下、誤った開示
   - E) 同上　苦情処理、受付ミス、受付への対応ミス
2. 個人データの安全管理に関するリスク
   - A) 正確性のリスク
     - ● 誤入力、誤配送　等
   - B) 個人データの安全管理のリスク
     - ① 機密性　盗難、窃視、不正なコピー
     - ② 完全性　改ざん、
     - ③ 可用性　破損、逸失
   - C) BYODによるリスク
     - ● ルール通りの運用の徹底
3. 電子保存3原則のリスク（真正性・見読性・保存性）
   - A) 自社内システムの安全管理・電子保存のリスク
   - B) クラウド（ASP含む）活用の際の安全管理・電子保存のリスク

追加：　プライバシーリスク
（ISO/IEC29134　より）
A) 過剰収集
B) 無許可リンク
C) 利用目的通知不足
D) 保管期間過剰
E) 開示権不足
F) 法的無権限処理
G) 同意不足利用・共有

参考：保健医療分野ガイダンス等

1．厚生労働省ホームページ

http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000027272.html

厚生労働分野における個人情報の適切な取扱いのためのガイドライン等

2．個人情報保護委員会ホームページ　　個人情報の適切な取扱いのためのガイダンス

https://www.ppc.go.jp/personal/legal/guidelines/#iryokanren（平成29年4月14日）

a．健康保険組合等における個人情報の適切な取扱いのためのガイダンス

b．国民健康保険組合における個人情報の適切な取扱いのためのガイダンス

c．国民健康保険団体連合会等における個人情報の適切な取扱いのためのガイダンス

3．個人情報保護委員会ホームページ　　「ガイドライン・QA等」の「その他」に掲載

https://www.ppc.go.jp/personal/legal/　（平成29年5月29日）

a．雇用管理分野における個人情報のうち健康情報を取り扱うに当たっての留意事項

4.個人情報保護の特別な分野の法

a．内閣府　医療分野の研究開発に資するための匿名加工医療情報に関する法律
（通称：次世代医療基盤法：認定匿名加工医療情報作成事業者の認定のための法律）

b．厚生労働省　臨床研究法（平成29年法律第16号）

http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000163417.html

5．研究に関する指針について：厚生労働省：改正個人情報保護法対応版：平成29年2月28日

http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/hokabunya/kenkyujigyou/i-kenkyu/

a．人を対象とする医学系研究に関する倫理指針
＋「医学研究のガイダンス」（正式名称：人を対象とする医学系研究に関する倫理指針ガイダンス）

b．ヒトゲノム・遺伝子解析研究に関する倫理指針

c．遺伝子治療等臨床研究に関する指針（改正個人情報保護法対応版：平成29年4月7日）

6．クラウドサービス事業者が 医療情報を取り扱う際の安全管理に関する ガイドライン

http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000209.html（平成 30 年7月 ）

✔ 安全管理に関する動向

- 安全管理ガイドライン改訂：Ver.5
- パスワードの変更

正確性・安全性の確保

法第十九条（**正確性**） 個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該 個人データを遅滞なく消去するよう努める。

→ 具体的なルールを策定　入力の確認のルール、誤配送の防止

→ 技術水準向上のための研究

法第二十条（**安全管理措置**）個人データの漏えい、滅失又はき損 の防止その他　の個人データの安全管理のために必要かつ適切な措置を講じる。

→ 機密性・完全性・保存性に関するリスク対策

法第二十一条（**従業者の監督**）個人データの安全管理が図られるよう、当該従業者に対する必要かつ適 切な監督を行わなければならない。

→　雇用契約・教育研修・監視・監督

法第二十二条（**委託先の監督**）個人データの取扱いの全部又は一部を委託する 場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行なう。

→　委託契約・派遣者の教育研修・委託先の監視・監督・再委託先管理

個人データに関する情報セキュリテイリスク対策

		正確性のリスク	安全管理のリスク		
			機密性に関するリスク	完全性に関するリスク	可用性に関するリスク
		誤入力、誤配送等	盗難、窃視、不正なコピー	改ざん	破損、逸失
安全管理措置	組織的対策	a. 個人情報保護に関する規程の整備、公表 、 b. 組織体制の整備、 c. 問題(緊急事態)発生時の報告・連絡体制の整備			
	物理的対策	a. 入退館管理(入退館記録・監視カメラ等による監視、検査の実施) b. 機器、装置などの盗難防止の固定、 c. BYOD(私物)機器の接続制限(有線・無線)			
	技術的対策	a. ユーザ登録、・アクセス権限付与、・アクセス記録の保存、 b. アクセス監視と管理、ソフトウエアの脆弱性対策			
従業者の監督		a. 雇用契約時の規程の整備 b. 適切な教育研修・適切な監視・監督(規則・罰則等)			
委託先の監督		a. 適切な委託先の選定・契約(特に、個人情報の適切な取扱い) b. 派遣者の場合は要員の適切な教育 c. 適切な監視・監督(規則・罰則等)、再委託先管理			

BYODの安全管理上の取扱い

1. BYOD取扱いの基本的な方針(例:私物ノートPC・スマホ・USB)

対象者	業務内容	対応
職員	個人保有	(健診現場含む)申請により持ち込み可とする。ただし、机の上に置かない等の制約はあり。
	業務保有	(健診現場含む)業務に必要な使い方を行う。
患者・受診者等	持ち込み・利用	可とするが、健診現場・診察室内等では利用を控えていただく
契約産業医等	持ち込み・利用	機関内・健診現場等で業務を行う人による外部機関データの持ち込み・利用は控える。(内部業務をする場所には持ち込み禁止)
外来作業者	データ入力・処理等	申請により持ち込み可とする

2. 利用可能区域(持ち込みは可能)

A) 通常職場内 不可、
B) 診察室・健診現場等、受診者(=顧客)と接する場所 不可
C) 廊下等 可

3. 個人所有のBYOD持ち込み承認

A) 職員:年1回申請、
B) パート:業務の開始日で最大1年、
C) 委託先で通常は機関内での作業:業務の開始日で最大1年
D) 委託先で納品・打ち合わせ時等にのみ機関内に入室

4. 個人所有の端末の業務利用の承認

A) 承認手続き B) 利用手順

BYOD:Bring Your Own Device

✓　産業保健分野の重要な改訂

A) 事業所内の個人健康情報の安全管理
法的守秘義務（医療職等）による人的対応

B) 個人健康情報の取扱いの職種による分担
働き方改革の個人健康情報の取扱い

a.　リスクへの対応：個人情報保護・安全管理

→ ガイドラインによりリスクへの具体的な対応を公表

b.　個人情報台帳の記載、

c.　取扱い担当者の設定：「医療職種」(新設)、「産業保健業務従事者」

- ✓　一般データ：法定のうち非医療情報
- ✓　心身的情報：法定のうち医療情報
- ✓　取扱いに本人の同意が必要：法定外の医療情報

A-a.事業所での雇用管理用個人健康情報の取り扱い

1.　安全管理に関して

「通則編」の「8.（別添）講ずべき安全管理措置の内容」への準拠を要求。

中小事業所向けは、特に、安全管理ガイドラインより少し緩和

⇒　現場状況にあわせた運用レベル(Windowsの最新updateやウイルスチェックソフト導入等)

2.　マネジメントするために

① 産業保健現場は事業所従業員の「要配慮個人情報」があるため、適切な個人情報保護方針を定めてマネジメントすることが望ましい。

② 保護すべき健康情報及びその管理運用責任を定義し、関係者全員が参照可能とする

3.　雇用管理用の個人健康情報は要配慮個人情報

取得・提供に、原則、**本人同意が必要**。（法律等に定められるものを除く）

しかし、医療職でなくても良い

4.　詳細な医学的情報の取扱い　⇒　産業保健業務従事者に行わせる

産業医・保健師等の 判断・意見、診断名、検査値、具体的な愁訴の内容等　加工前の情報

⇒　本人から開示請求があった場合は、原則として開示

5. ストレスチェックの「実施者」本人の同意を得ないで結果を事業者に提供不可

「実施者」 ⇒　医師、保健師その他 厚労省令で定める

A-b. 雇用管理に関する健康情報の取扱い

1. **「雇用管理分野における個人情報のうち健康情報を取り扱うにあたっての留意事項」**（厚生労働省　2017年5月制定）
   http://www.mhlw.go.jp/file/06-Seisakujouhou-12600000-Seisakutoukatsukan/0000167762.pdf
   雇用管理の際の安全管理に関するガイドライン
   → 個人情報保護ガイドライン（通則編）を適用することが明記。

2. 神奈川労働局より**「安衛法、改正・個人情報保護法、個人情報ガイドラインとの突合表」が公表された。**
   https://jsite.mhlw.go.jp/kanagawa-roudoukyoku/var/rev0/0119/9543/201792082314.pdf
   「留意事項」と「ガイドライン」の対応が分かりやすくなっている。
   https://jsite.mhlw.go.jp/kanagawa-roudoukyoku/var/rev0/0119/9542/201792082252.pdf

3. **ストレスチェック情報の取扱い**　「雇用管理・・・・留意事項」の3ページ
   （3）安衛法第 66 条の 10 第2項において、ストレスチェックを実施した医師、保健師その他の厚生労働省令で定める者（以下「実施者」という。）は、**労働者の同意を得 ないでストレスチェック結果を事業者に提供してはならない**こととされており、事業者は、実施者又はその他のストレスチェックの実施の事務に従事した者（以下「実施事務従事者」という。）に提供を強要する又は労働者に同意を強要する等の不正の 手段により、労働者のストレスチェックの結果を取得してはならない。

B-a.高度プロフェッショナル(働き方改革)に対する産業医・産業保健機能の強化

労働安全衛生法改正事項の内容（2019年4月施行予定）

1. 事業者による産業医に対する情報提供

   労働時間数を超える労働者の氏名、業務内容その他、産業医が労働者の健康管理等を適切に行うために必要な情報

2. 産業医による勧告と事業者の対応

   勧告の内容その他厚生労働省令で定める事項を衛生委員会又は安全衛生委員会に報告する義務

3. 産業医の業務内容を労働者へ衛生管理者等へ周知

   a. 長時間労働の医師の面接指導

   b. 医師の面接指導の義務化

      - 新たな技術、商品又は役務の研究開発に係る業務につく労働者
      - 特定高度専門業務・成果型労働制の対象労働者

   c. 事業者による労働時間把握の義務化

   d. 労働者の心身の情報に関する取り扱い

労働安全衛生法が改正されるとともに、ガイドライン発行予定
https://www.mhlw.go.jp/topics/bukyoku/soumu/houritu/dl/196-31.pdf
働き方改革実行計画を踏まえた今後の産業医・産業保健機能の強化について（報告：事務局案）

d）改正労働安全衛生法

現行

第104　第65条の2第1項及び第66条第1項から第4項までの規定による健康診断、第66条の8第1項の規定による面接指導、第66条の10第1項の規定による検査又は同条第3項の規定による面接指導の実施の事務に従事した者は、その実施に関して知り得た労働者の**秘密を漏らしてはならない。**

安全管理リスクへの対応

個人情報保護リスクへの対応

改正後

第104条　事業者は、この法律又はこれに基づく命令の規定による措置の実施に関し、労働者の心身の状態に関する情報を収集し、保管し、又は使用するに当っては、労働者の健康の確保に必要な範囲内で労働者の心身の状態に関する情報を収集し、並びに当該**収集の目的の範囲内でこれを保管し、及び使用しなければならない。**ただし、本人の同意がある場合その他正当な事由がある場合は、この限りでない。

２ 事業者は、労働者の心身の状態に関する情報を適正に管理するために必要な措置を講じなければならない。

３ 厚生労働大臣は、前二項の規定により事業者が講ずべき措置の適切かつ有効な実施を図るため**必要な指針を公表する**ものとする。

４ 厚生労働大臣は、前項の指針を公表した場合において必要があると認めるときは、事業者又はその団体に対し、当該指針に関し必要な指導等を行うことができる。

ガイドラインによりリスクへの具体的な対応を公表

f） 労働者の心身の状態に関する情報の適正な取扱いのために事業者が講ずべき措置に関する指針（案）

1　趣旨・総論

事業者が、労働安全衛生法（昭和 47 年法律第 57 号）に基づき行う健康診断等の健康確保措置や任意に行う労働者の健康管理活動を通じて得た労働者の心身の状態に関する情報（以下「心身の状態の情報」という。）については、そのほとんどが個人情報の保護に関する法律（平成 15 年法律第 57 号）第２条第３項に規定される**「要配慮個人情報」に該当するなど機密性が高い情報**である。そのため、事業場において、労働者が雇用管理において自身にとって不利益な取扱いを受けるという不安を抱くことなく、安心して産業医等による健康相談等を受けられるようにするとともに、事業者が必要な心身の状態の情報を取得して、労働者の健康確保措置を十全に行えるようにするために、関係法令に従った上で、心身の状態の情報が適切に取り扱われることが必要であり、当該事業場における心身の状態の情報の適切な取扱いのための規程（以下「取扱規程」という。）の明確化が必要である。よって、本指針においては、心身の状態の情報の取扱いに関する原則を明らかにしつつ、事業者が策定すべき規程の内容、策定の方法、運用等について示すこととする。

個人情報保護リスクへの対応

g） 労働者の心身の状態に関する情報の適正な取扱いのための指針（案）

２　心身の状態の情報の取扱いに関する原則

（３）取扱規程に定めるべき事項

事業場ごとに取扱規程に定めるべき事項は具体的に以下のものが考えられる。

なお、心身の状態の情報を取り扱う者及びその権限については、個々の事業場において心身の状態の情報の取り扱う目的や取り扱うための体制等の状況に応じて、部署や職種ごとに、その権限及び取り扱う心身の状態の情報の範囲等を定めることが必要。

① 心身の状態の情報を取り扱う目的及び取扱い方法
② 心身の状態の情報を取り扱う者及びその権限並びに取り扱う心身の状態の情報の範囲
③ 心身の状態の情報を取り扱う目的等の通知方法及び本人同意の取得方法
④ 心身の状態の情報の適正管理
⑤ 心身の状態の情報の開示、訂正等及び使用停止等の方法（消去に関するものを含む。）
⑥ 心身の状態の情報の第三者提供
⑦ 事業承継、組織変更に伴う心身の状態の情報の引継ぎに関する事項
⑧ 心身の状態の情報の取扱いに関する苦情の処理
⑨ 取扱規程の労働者への周知の方法

（５）心身の状態の情報の適正な取扱いのための体制の整備

・・・なお、健康診断の結果等の記録データについては、事業者の責任の下で、健康診断を実施した医療機関等と連携して加工や保存を行うことも考えられるが、その場合においても、取扱規程においてその取扱いを定めた上で、健康確保措置を講じるために必要な心身の状態の情報は事業者が把握し得る状態に置く等の必要がある。

個人情報台帳の記載

取扱い担当者の明確化

h） 心身の状態の情報の取扱いに係る法令等との整理

① 労働安全衛生法令において事業者が直接取り扱うこととされており、事業場ごとの取扱規程により事業者の取扱いを制限することが想定されていない心身の状態の情報：

(a)健康診断の受診・未受診の情報
(b)長時間労働者による面接指導の申出
(c)ストレスチェックの結果高ストレスと判定された者による面接指導の申出
(d)健康診断等の事後措置に関する医師の意見

一般データ：
法定のうち
非医療情報

② 労働安全衛生法令において事業者が本人の同意を得なくても取得することが可能であるが、事業場ごとの取扱規程により事業者の取扱いを制限することが適当である心身の状態の情報：

(a)健康診断の結果（法定項目）
(b)健康診断の再検査の結果（法定の健康診断項目と同一のものに限る。）
(c)長時間労働者に対する面接指導の結果
(d)ストレスチェックの結果高ストレスと判定された者に対する面接指導の結果

心身的情報：
法定のうち
医療情報

③ 労働安全衛生法令において事業者による取扱いについて規定されていないため、取得する段階で事前に本人の同意を得ることが必要となるとともに、事業場ごとの取扱規程により、適正に取り扱う必要のある心身の状態の情報：

(a)健康診断の結果(法定外項目)
(b)保健指導の結果
(c)健康診断の再検査の結果（法定の健康診断項目と同一のものを除く。）
(d)健康診断の精密検査の結果
(e)健康相談の結果
(f)がん検診の結果
(g)職場復帰のための面接指導の結果
(h)治療と仕事の両立支援等のための医師の意見書

取扱いに本人の
同意が必要：
法定外の
医療情報

i) 労働者の心身の状態に関する情報の適正な取扱いのための指針（案）

4 定義

「心身の状態の情報」

・・・労働安全衛生法・・・に基づく健康診断等の健康確保措置や任意に行う労働者の健康管理活動を通じて得た情報であり、このうち個人情報の保護に関する法律第2条第3項に定める「要配慮個人情報」に該当するものについては、「雇用管理分野における個人情報のうち健康情報を取り扱うに当たっての留意事項」の「健康情報」と同義である。・・・

「心身の状態の情報の加工」

心身の状態の情報の他者への提供に当たり、提供する情報の内容について、健康診断の結果等の記録データそのものではなく、所見の有無や検査結果を踏まえた就業上の措置に係る医師の意見に置き換えるなど、当該心身の状態の情報の取扱いの目的の達成に必要な範囲内で使用されるように変換することをいう。

・心身的情報：法定のうち医療情報
・法定外の医療情報

「医療職種」

医師、保健師等、法律において、業務上知り得た人の秘密について守秘義務規定が設けられている職種をいう。

「産業保健業務従事者」

医療職種や衛生管理者その他の労働者の健康管理に関する業務に従事する者をいう。

別表1：産業医の付加業務として
依頼される可能性のある職務

＜取扱注意＞

1　労働安全衛生法関連の職務

① 健康診断の実施
② ストレスチェックの実施
③ 健康診断の問診や診察等の医療記録を保存
④ 面接指導の記録を保存
⑤ ストレスチェック結果の集団分析
⑥ 衛生教育

労働安全衛生法

2　労働安全衛生法に規定されていない職務

① 診断書その他の健康情報を解釈し人事管理に活用
② 労働者からの健康相談対応
③ 職場復帰の可否を判断と支援
④ 事業場滞在中に発生した急患への救急処置
⑤ 運転業務等の特殊職務に従事する労働者の就業適性の診断
⑥ 健康教育等の健康保持増進活動の実施
⑦ 感染症を予防と発生後の拡大防止
⑧ 作業環境測定結果を確認と職場改善等の意見陳述
⑨ 職場や作業の快適化に関する助言
⑩ 危険有害要因のリスクアセスメントに関する助言
⑪ 労働衛生関連訴訟に関する助言
⑫ 事故又は災害が発生後の被害最小化策に関する助言

医療法・医師法

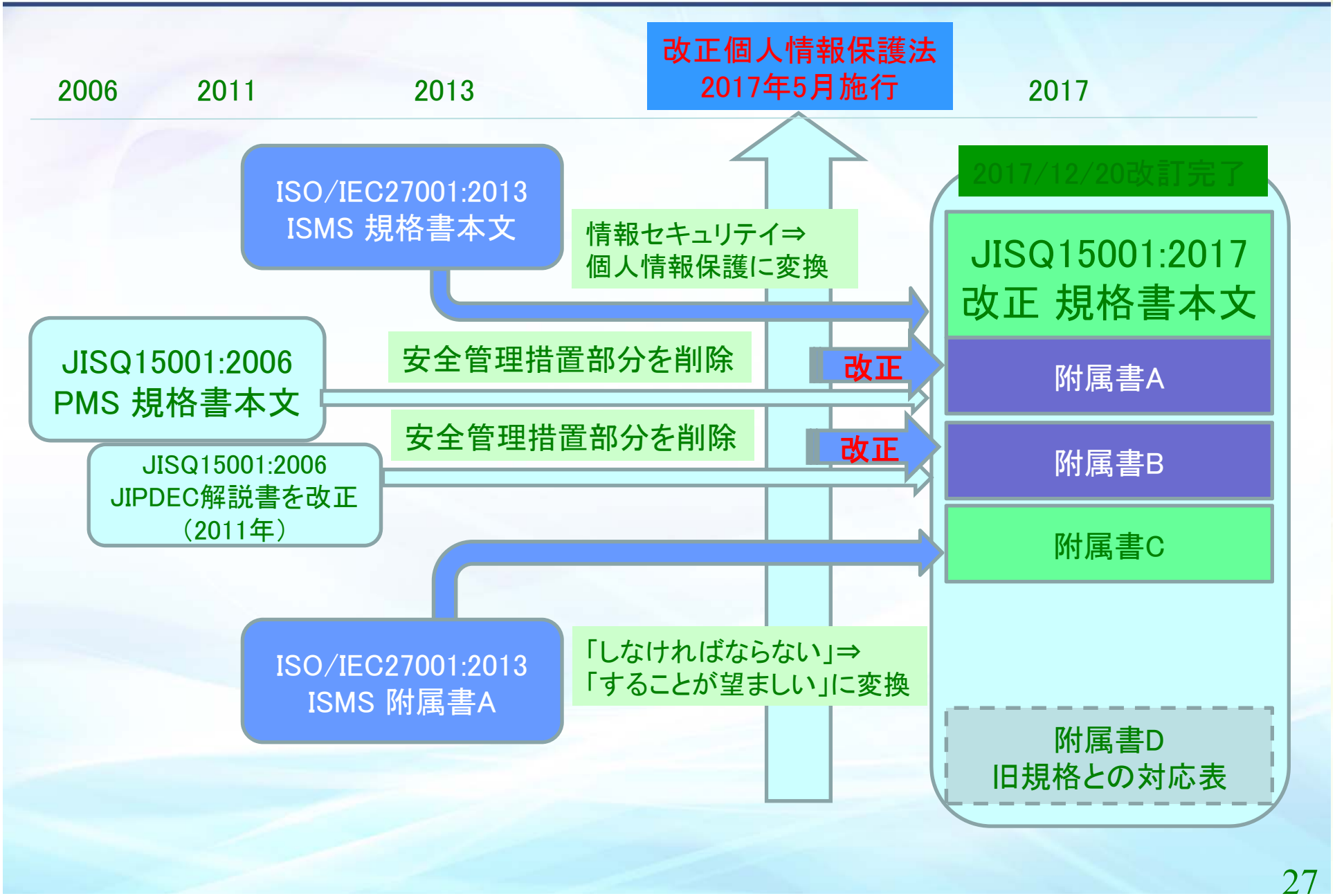
3　労働安全衛生以外の職務

① 職場での患者の診療
② 顧客の健康を確保する活動に参画すること
③ 医療保険者による保健事業（特定健康診査、データヘルス活動等）に協力すること
④ 関連協力企業又は構内請負企業において産業医の職務を行うこと
⑤ 国、地方公共団体、学術団体その他の公益事業に協力すること

（JISQ15001 ：全体の復習）.

JISQ15001:2017の規格改正の経緯と対応案

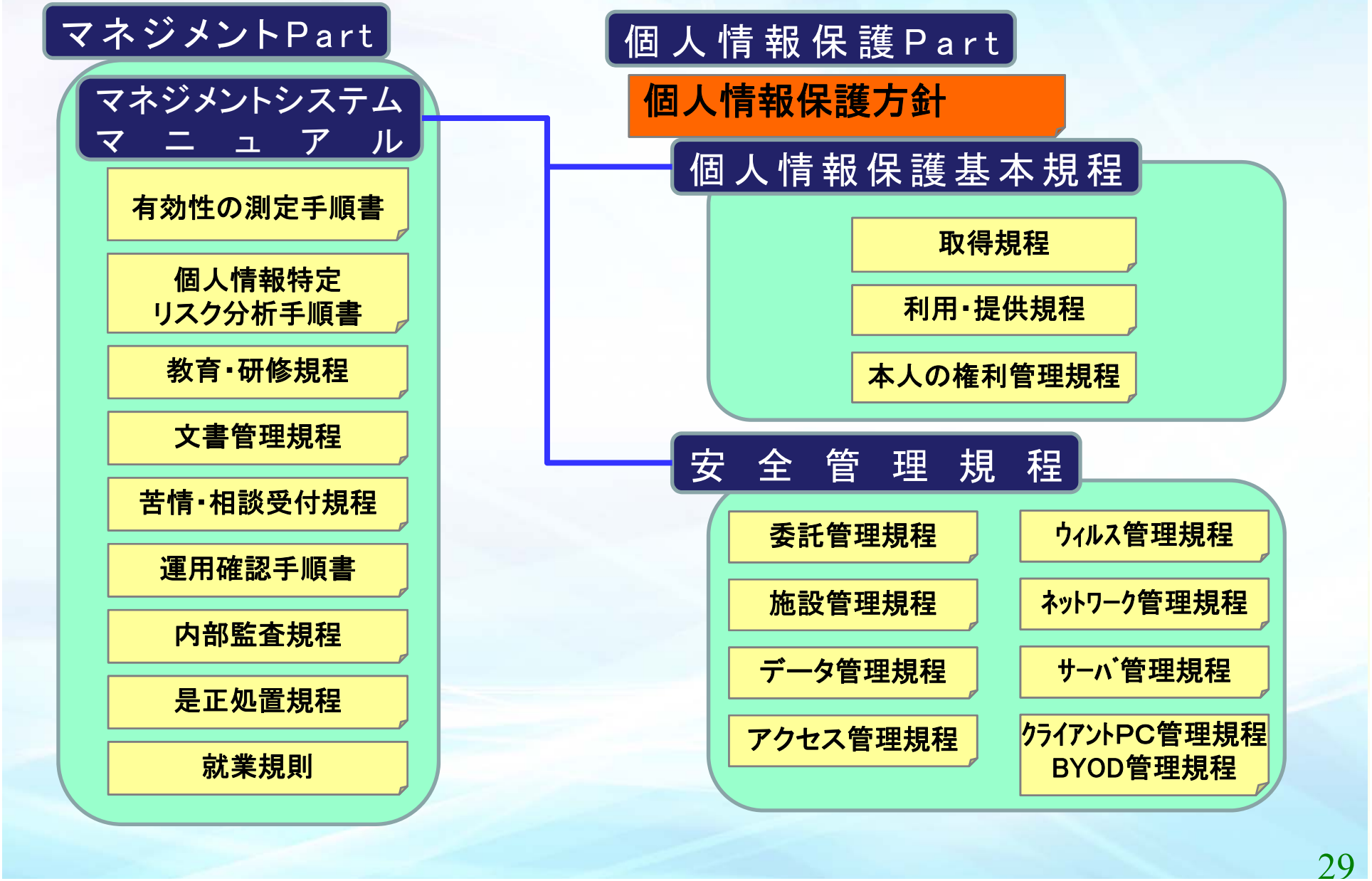
JISQ15001規格改正による構成変更の概要



新JISQ15001におけるパフォーマンス評価

新JISQ15001:2017	旧JISQ15001:2006
1 適用範囲、2 引用規格	**1 適用範囲**
3 用語及び定義、4 組織の状況	**2 用語及び定義**
4.1 組織及びその状況の理解	3.3.2 法令，国が定める指針その他の規範
4.3 個人情報保護マネジメントシステムの適用範囲の決定	3.3.1個人情報の特定
4.4 個人情報保護マネジメントシステム	3 要求事項 3.1 一般要求事項
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	3.3.4 資源.役割，責任及び権限
5.2 方針	3.2 個人情報保護方針
5.3 組織の役割，責任及び権限	3.3.4 資源.役割，責任及び権限(再掲)
6 計画	**3.3 計画**
6.1 リスク及び機会に対処する活動	3.3.5 内部規程、3.3.3 リスクなどの認識，分析及び対策
6.2 個人情報保護目的及びそれを達成するための計画策定	3.3.6 計画書
7 支援	
7.1 資源、7.2 力量	3.3.4 資源，役割，責任及び権限
7.3 認識、7.4 コミュニケーション	3.4.5 教育、3.3.7 緊急事態への準備
7.5 文書化した情報	3.5 個人情報保護マネジメントシステム文書
8 運用	**3.4 実施及び運用**
8.1 運用の計画及び管理	3.4.1 運用手順
8.3 個人情報保護リスク対応	
A.3.4.2.2 適正な取得	3.4.2.2 適正な取得
A.3.4.2.6,7,8 利用、連絡又は接触、提供	3.4.2.6 利用、アクセス、提供
A.3.4.3 適正管理	3.4.3_適正管理
A.3.4.4 個人情報に関する本人の権利.	3.4.4 個人情報に関する本人の権利
A.3.6 苦情及び相談への対応	3.6 苦情及び相談への対応
9 パフォーマンス評価	**3.7 点検**
9.1 監視，測定，分析及び評価、	3.7.1 運用の確認
9.2 内部監査、	3.7.2 監査
9.3 マネジメントレビュー、	3.9 事業者の代表者による見直し
10. 改善	**3.8 是正処置及び予防処置**
10.1 不適合及び是正処置、	
10.2 継続的改善	

個人情報保護マネジメントシステムの構造



I) .個人情報DB、個人データ、保有個人データに対する事業者の義務

「事業者の義務」

個人情報
生存する個人に関する情報

1. 利用目的の特定
2. 利用目的の通知
3. 適正な取得
13. 理由説明と苦情対応

個人情報データベース
個人情報を一定の規則(例えば、五十音順、生年月日順など)に従って整理・分類し、特定の個人情報を容易に検索することができるよう、体系的に構成した情報の集合物

匿名加工情報データベース
匿名加工情報の集合物

3. 正確性確保
4. 安全管理
5~8. 第三者提供

個人データ
個人情報データベース等を構成する個人情報

匿名加工情報
特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにした情報

保有個人データ
医療機関が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データ

9. 保有個人データに関する事項の公表
10. 開示
11. 訂正・停止
12. 開示手続と手数料

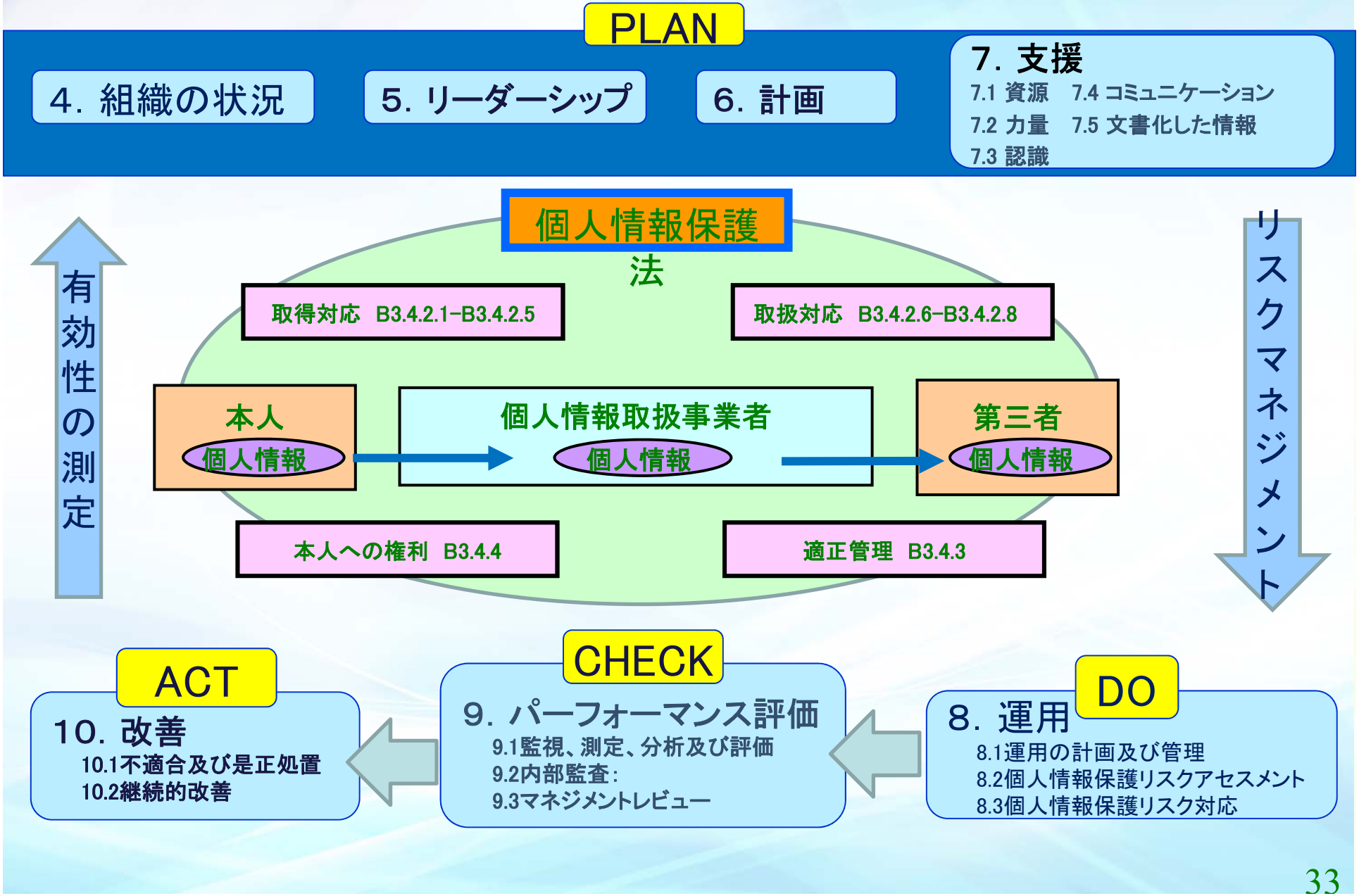
個人情報の定義、個人情報の特定

新PマークJISQ15001:2017 B.3.3.1個人情報の特定(本文の要約)	旧PマークJISQ 15001:2006 2. 用語の定義(個人情報に関連する条項)
a. ”社会通念上、特定の個人を識別できる”と判断	2. 1　個人情報
一般人の判断力又は理解力をもって生存する具体的な人物と当該情報との間に個人識別性を認めるに至ることができるかどうかを考慮して判断する。	**個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述などによって特定の個人を識別できるもの**(他の情報と容易に照合することができ、それによって、特定の個人を識別できることとなるものを含む。)。
b.「個人情報」に該当するかどうかの判断は A.3.3.2 に基づいて行う。	
c. **死者の情報も対象とすることが望ましい**理由 ・死者の情報の適正な取扱いと管理が必要であると判断される場合 ・故人の個人情報が遺族の個人情報として解されることがある。 ・その利用目的との関係において，生死の別を厳格に管理しない場合もある。 ・事業活動においては，契約によって取得している個人情報も多く，その一方当事者の即時に個人情報保護マネジメントシステムの対象情報から除外するというものでもない。 ・死者の情報には，歴史上の人物まで対象とする必要がない。	「解説」より **”個人情報”には、死者の情報も含まれる**が、歴史上の人物まで対象となるものではない。 2. 2　本人 個人情報によって識別される特定の個人。
d. **組織は，事業において利用する全ての個人情報について台帳整備が必須であるというわけではなく，** また，個人情報の取扱いについては，その個人情報の利用目的を特定した上で，その利用目的の範囲内で，個人情報保護リスクに応じて個々の従業者にゆだねるなど，柔軟な取扱いとしてもよい。	**3.3.1 個人情報の特定** 事業者は，自らの事業の用に供するすべての個人情報を特定するための手順を確立し，かつ，維持しなければならない。
e. **“組織は，特定した個人情報については，個人データと同様に取扱わなければならない。”** A.3.4.2、A.3.4.3 において個人データに対する管理策だけが示される場合であっても，特定した個人情報については，A.3.3.3 に基づき個人情報保護リスクに応じて，必要かつ適切な安全管理措置を講じることをいう。	

J)-1法律上の個人情報と個人データ

1. 「個人データ」 法律上の安全管理の義務あり
2. 今後は匿名化しても同様
3. JISQ15001では、
   a. 個人情報のうち、「**個人情報として特定したものは、個人データと同じ扱い**」とする。
   b. 匿名化・匿名加工情報も個人情報台帳に記載する
   c. 個人データの事例
      - 個人情報データベース等から外部記録媒体に保存された個人情報
      - 個人情報データベース等から紙面に出力され帳票等に印字された個人情報
   d. 個人情報台帳に掲載しない
      → 社内野球部の名簿
      → 個人収集の名刺
      → 電話メモ
      → （歴史上の人物）徳川家の家系図、百人一首の作者一覧

JISQ15001の本文（MSS共通要素の枠組み）



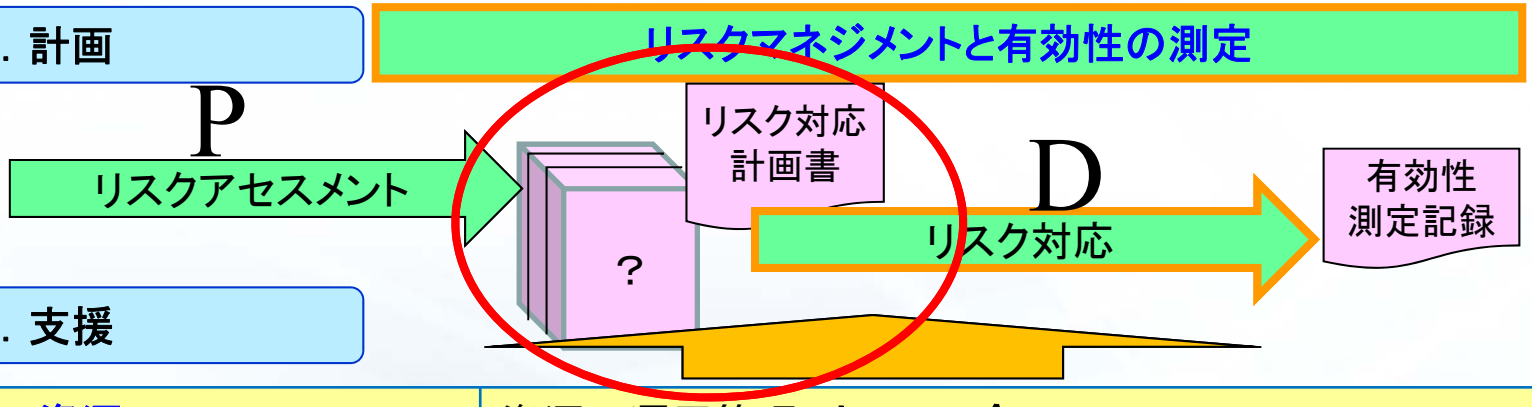
リーダーシップ・計画・支援

情報セキュリティ基本方針
個人情報保護方針

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 方針
5.3組織の役割、責任及び権限

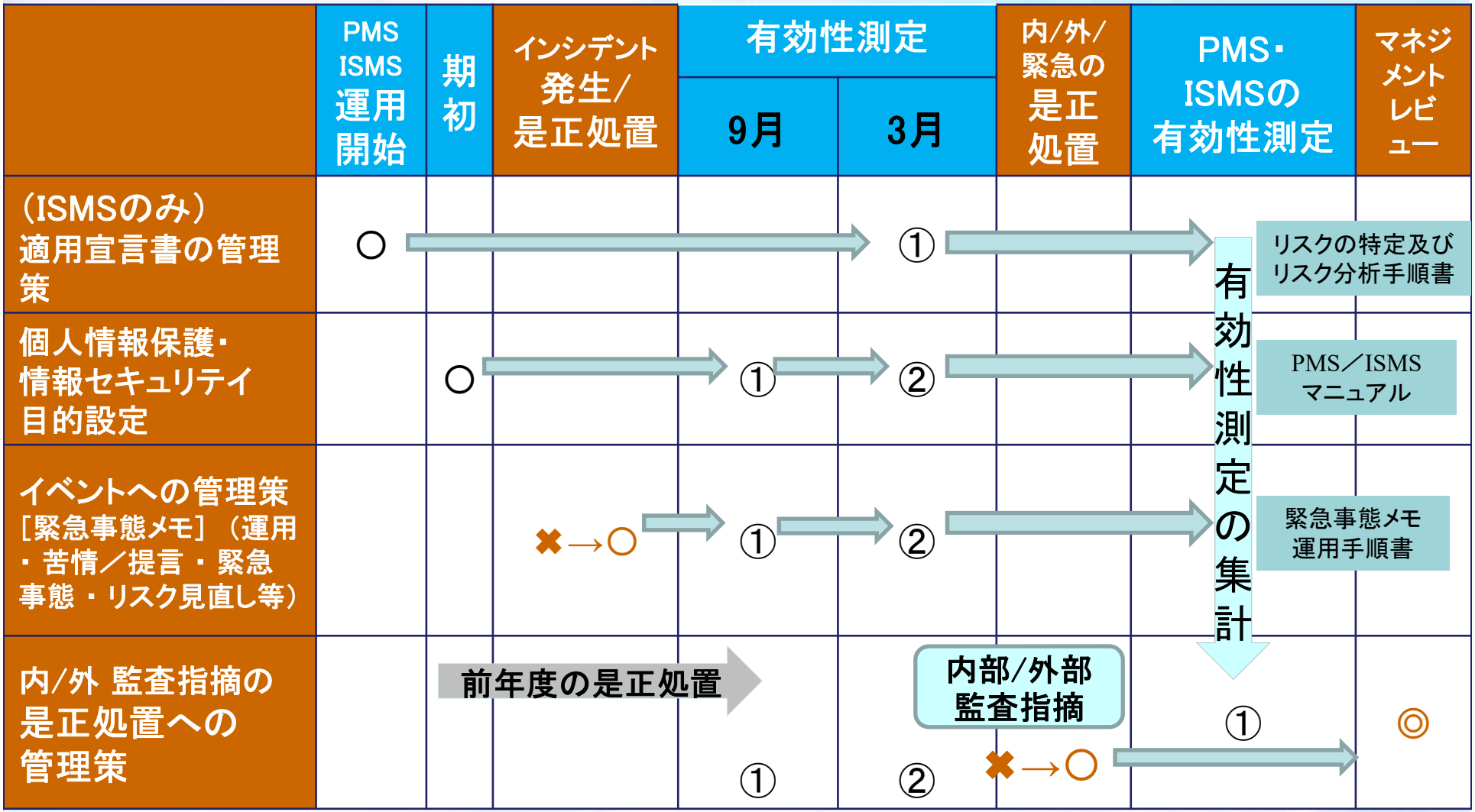
6. 計画



7. 支援

7.1 資源	資源の運用管理：人・モノ・金
7.2 力量	職員の教育：一般職員・管理者・内部監査員等
7.3 認識	職員の認識向上：方針・有効性への役割・不適合の意味
7.4 コミュニケーション	必要性：内容・実施時期・対象者・実施者・実施プロセス
7.5 文書化した情報	規程及び記録様式の制定・配布

有効性の評価項目と評価計画
（ISMSの場合、測定項目と測定計画）



「個人情報保護目的」の考え方

6.2 個人情報保護目的及びそれを達成するための計画策定

次の事項を満たす、個人情報保護目的を確立

a) 内部向け個人情報保護方針と整合している。
b) （実行可能な場合）測定可能である。
c) 適用される個人情報保護要求事項，
　並びにリスクアセスメント及びリスク対応の結果を考慮に入れる。
d) 伝達する。
e) 必要に応じて，更新する。

個人情報保護目的とは
こんなもの

個人情報保護目的の達成計画を立てる。

f) 実施事項
g) 必要な資源（担当者・実施分担）
h) 責任者（責任部署の明確化）
i) 達成期限（期限及び期末ごとのチェック内容）
j) 結果の評価方法（「達成」と評価すべき状態は？）

左記項目を含む
達成計画を作る

「個人情報保護目的」の考え方

「個人情報保護目的」の「目的」を「目標」に引き比べて説明

（ISO/IEC27001　情報セキュリテイマネジメント　JIPDEC刊より）

1. 目標は目的を達成するためにある。
2. 目的は抽象的でよいが、目標は具体的でなければならない。
3. 目的は行き先であり、目標は過程である。
4. 一つの目的には、複数の目標がある。
5. 目標はあきらめることがあるが、目的はあきらめてはいけない。

注：3.8 目的 達成する結果。（注：JISQ15001：2017 「3. 用語の定義」より）

注記 1 目的は，戦略的，戦術的又は運用的であり得る。
注記 2 目的は，様々な領域（例えば，財務，安全衛生，環境）の到達点に関連し得るものであり，様々な階層［例えば，戦略的レベル，組織全体，プロジェクト単位，製品ごと，プロセス（3.12）ごと］で適用できる。
注記 3 目的は，例えば，予定された成果，意図，運用基準など，別の形で表現することもできる。また，個人情報保護目的という表現の仕方もある。又は，同じような意味をもつ別の言葉（例 狙い，到達点，目標）で表すこともできる。
注記 4 個人情報保護マネジメントシステムの場合，組織は，特定の結果を達成するため，内部向け個人情報保護方針と整合のとれた個人情報保護目的を設定する。

3. パフォーマンスを向上するために（上級編）

8. 運用

8.1 運用の計画及び管理

8.2 個人情報保護リスクアセスメント

8.3 個人情報保護リスク対応

8 運用 8.1 運用の計画及び管理

個人情報保護要求事項，及び リスク対応計画の策定・実施・管理	
	個人情報保護要求事項を満たすため，及び 6.1 で決定した（リスク対応の）活動を実施するために必要なプロセ スを計画し，実施し，かつ，管理する。
個人情報保護目的の計画と実施	
	6.2 で決定した個人情報保護目的を達成するための計画を実施しなければならない。 組織は，プロセスが計画通りに実施されたという確信をもつために必要な程度の，文書化した情報を保持する。
有効性測定計画の策定・管理	
	計画通りに実施された（有効であった）という確信をもつために必要な程度の，文書化した情報を保持する。
リスク対応計画と有効性測定計画の変更管理	
	計画した変更を管理し，意図しない変更によって生じた結果をレビューし，必要に応じて，有害な影響を軽減する処置を行う。
外部委託の決定・変更管理	
	外部委託したプロセスが決定され，かつ，管理されていることを確実にする。

現場管理者による監視の実務(1)
JISQ15001　附属書A　A.3.7.1 運用の確認

1. PMSが適切に運用されていることが
   ・組織の各部門及び階層において
   ・定期的に，及び適宜に確認されるための
   ・手順を確立し，実施し，かつ，維持する。

   a. 各部門の管理者は，定期的に，及び適宜に運用状況を確認する。

   b. 個人情報保護管理者は，代表者に，定期的に，及び適宜に代表者にその状況を報告する。

2. 確認する項目は、様々な理由により、リスク対策にもかかわらず残留リスクがある部分。

   a. 安全管理ガイドラインの「C項」（必須事項）を参照し、対応不十分な場合

   b. この他に、取得・利用・提供等、個人情報保護に関する残留リスクにも注目

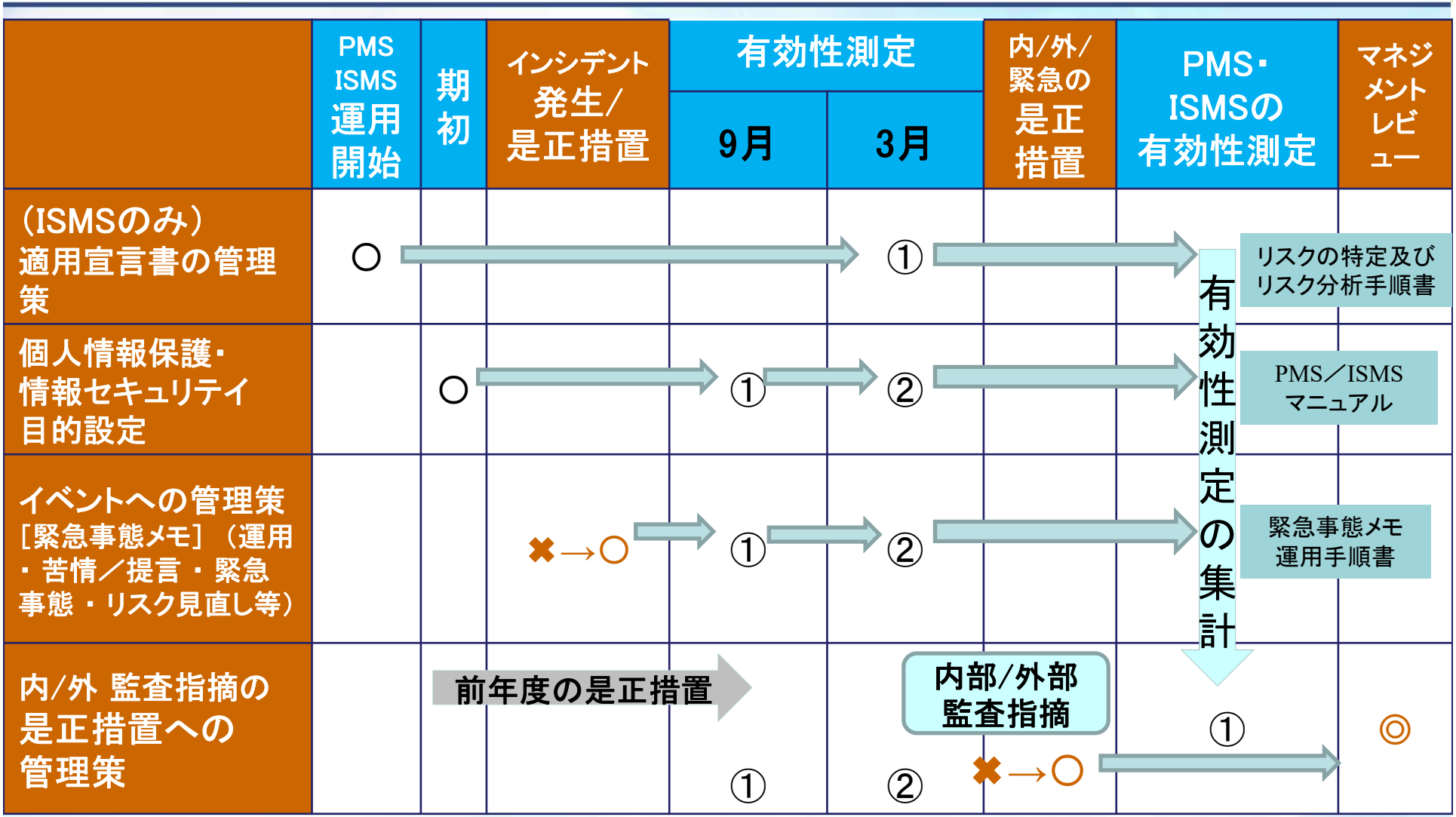
現場管理者による監視の実務(2)
参考：安全管理GL　C項より

- PMSのマネジメントシステムのパフォーマンス及び有効性を評価するために次の事項を行う。
  - a）予算実績の分析・評価（毎月）
  - b）外部監査（実施時期は監査内容に従う）
    - ①PMSプライバシーマーク審査（ 1回／2年）
  - c）内部監査（毎年？？月）
  - d）個人情報保護目的に対する各部の分析・有効性の評価
    - ［毎年？？月(中間)・？？月］
  - e）トラブル報告書の分析・有効性の評価
    - ［随時かつ全体評価は毎年1月に実施］
  - f）管理策の有効性評価（年1回）
  - g）外部委託業務評価（年1回）
  - i）マネジメントレビュー（年1回）

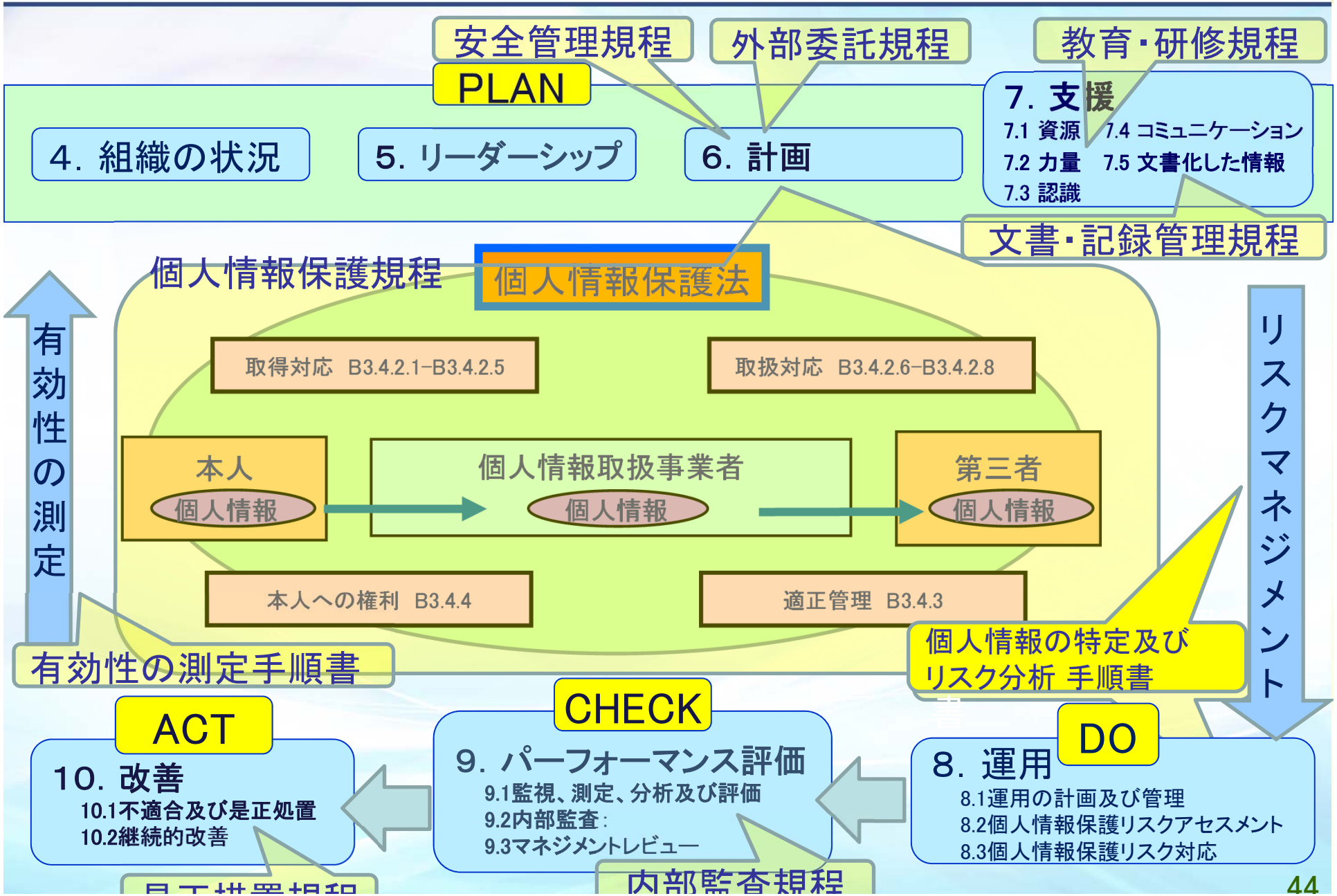
これらの監視が手順書等に基づき、実施されていることを監査員jが確認する

対応すべき詳細規程：「PMSマニュアル」「運用確認手順書」「内部監査規程」「苦情相談受付規程」「有効性測定手順書」

有効性の評価項目と評価計画
（ISMSの場合、測定項目と測定計画）



JISQ15001の MSS共通要素の枠組み



8.2 個人情報保護アセスメント、8.3 リスク対応

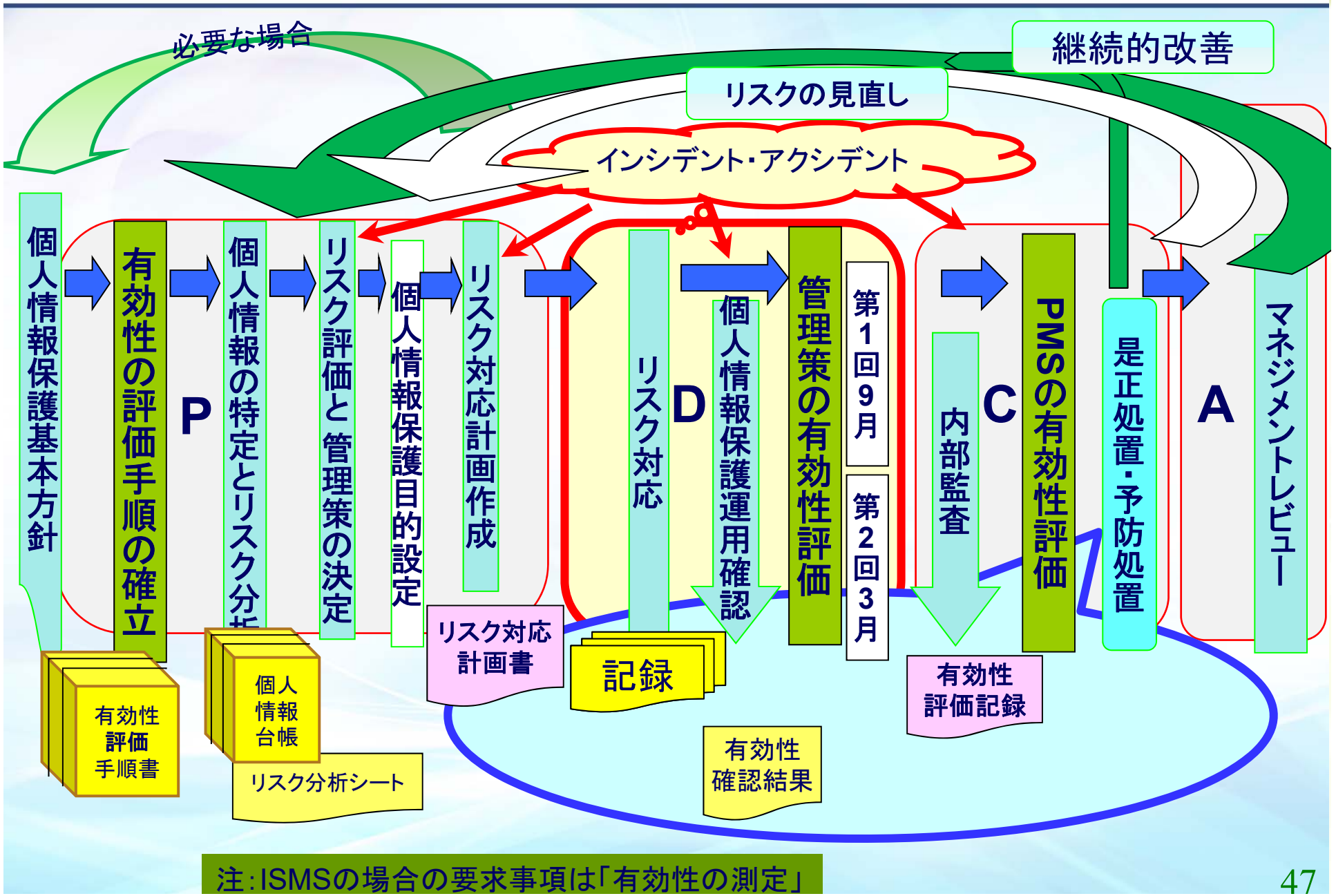
1. 個人情報保護リスクアセスメントの実施
   ① 基準を考慮[6.1.2.1 a)で確立する]して、
      ① あらかじめ定めた間隔
      ② 重大な変更が提案された
      ③ 若しくは、重大な変化が生じた場合
2. 個人情報保護リスクアセスメント結果の文書化した情報の保持
3. 有効性の評価の確認

4. 個人情報保護リスク対応計画の実施
5. 個人情報保護リスク対応結果の「文書化した情報」の保持

パフォーマンス評価と改善の旧JISからの対応

新JIS	旧JIS
9 パフォーマンス評価 A.3.7 パフォーマンス評価	3.7 点検
9.1 監視，測定，分析及び評価、 A.3.7.1 運用の確認	3.7.1 運用の確認
9.2 内部監査、 A.3.7.2 内部監査	3.7.2 監査
9.3 マネジメントレビュー、	3.9 事業者の代表者による見直し
10. 改善	3.8 是正処置及び予防処置
10.1 不適合及び是正処置、	
10.2 継続的改善	

（PMS運用時の）リスクマネジメントと有効性評価



9.1 監視，測定，分析及び評価

組織は，個人情報保護パフォーマンス及び個人情報保護マネジメントシステムの**有効性を評価**しなければならない。
組織は，次の事項を決定しなければならない。

A) 必要とされる監視及び測定の対象。これには，個人情報保護プロセス及び管理策を含む。
B) 該当する場合には，必ず，妥当な結果を確実にするための，監視，測定，分析及び評価の方法

注記：選定した方法は，妥当と考えられる，**比較可能で再現可能な結果を生み出すこと**が望ましい。

C) 監視及び測定の実施時期
D) ――――――――実施者
E) ――――――――結果の，分析及び評価の時期
F) ――――――――結果の，分析及び評価の実施者

組織は，監視及び測定の結果の証拠として，適切な文書化した情報を保持しなければならない。

緊急事態への管理策

事象

- 1群. 運用・緊急事態・苦情/提言・リスク見直し
- 2群. 内部及び外部の監査

是正処置

管理策

A.16.1 インシデントの管理及びその改善
責任及び手順
事象
弱点の報告
事象の評価及び決定
インシデントへの対応
インシデントからの学習
証拠の収集

A.17.1 事業継続
事業継続の計画
事業継続の実施
事業継続の検証, レビュー及び評価

A.17.2 冗長性
弱点の報告

実施した管理策の有効性測定

JISQ15001 付属書CよりMPO作成

10. 改善

内部監査と是正処置

1. ISO 19011:2011：監査の為の指針
「監査基準が満たされている程度を判定するために、監査証拠を収集し、それを客観的に評価するための体系的で、独立し、文書化されたプロセス」

ISMS・QMS等（共通規格）における予防処置の用語の廃止
2. → JISQ15001:2017も予防処置を廃止

3. 是正処置：
a. 不適合として指摘された、そのものの是正
b. 原因の追求
c. 再発防止策
d. 発生可能性の検討

予防処置の廃止の一方、
是正処置に関連して
①リスク分析見直し
②有効性の評価

不適合及び是正処置と他部門への展開

C

不適合!

1. 是正の実施
   a) 必要な処置の実施
   b) 是正処置の有効性をレビュー

■不適合を管理・是正のための処置
■不適合がもたらした結果への対処

2. 規程等の変更（必要な場合）

3. 不適合の再発又は他所での発生を防止する処置の必要性を評価
1) 不適合のレビュー
2) 不適合の原因の明確化
3) 類似の不適合の有無，又は発生可能性の明確化

■検出された不適合のもつ影響に応じた是正処置を実施

4. 処置内容の記録 ■ エビデンスとして，下記の文書化情報を保持:
・不適合の性質及びとった処置（が適正だったか？）、・是正処置の結果（は良好か？）

2つの規格での是正処置は中身が同じ
ISO/IEC27001: 10.1 JISQ15001: 10.1

9.3 マネジメントレビューの考慮事項

a) 前回までのマネジメントレビューの結果とった処置の状況

b) PMSに関連する外部及び内部の課題の変化

c) 次に示す傾向を含めた，情報セキュリティパフォーマンスに関するフィードバック

1) 不適合及び是正処置
2) 監視及び測定の結果
3) 監査結果
4) 情報セキュリティ目的の達成

監査結果の活用

d) 利害関係者からのフィードバック

e) リスクアセスメントの結果及びリスク対応計画の状況

f) 継続的改善の機会

9.3 PMSによる代表者による見直し概要

見直しへのインプット

PMS見直し報告書

1年に1回以上実施

代表者の見直し

個人情報保護責任者が取りまとめ
代表者に報告、レビューする。

見直しからのアウトプット

PMS見直し計画書

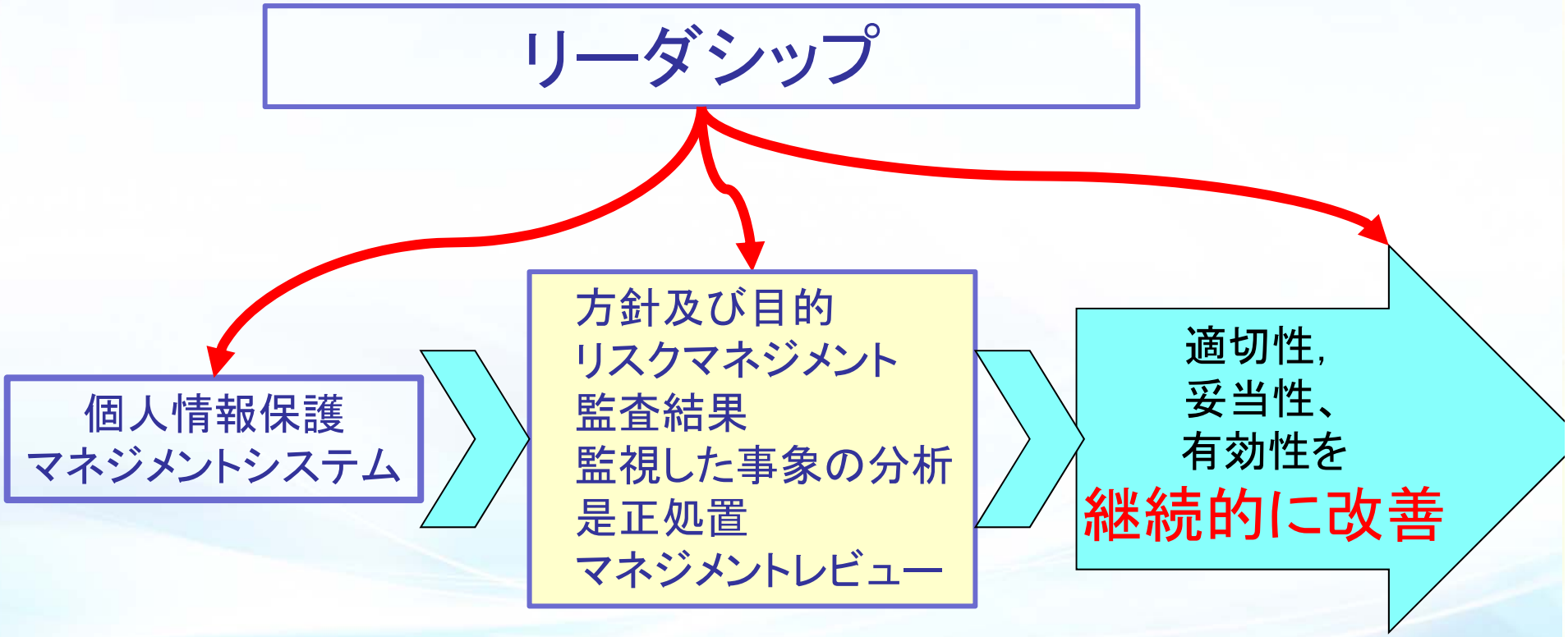
a) 前回までのマネジメントレビューの結果，とった処置の状況
b) 個人情報保護マネジメントシステムに関連する外部及び内部の課題の変化
c) 次に示す傾向を含めた，個人情報保護パフォーマンスに関するフィードバック
1) 不適合及び是正処置
2) 監視及び測定の結果
3) 監査結果
4) 個人情報保護目的の達成
d) 利害関係者からのフィードバック
e) リスクアセスメントの結果及びリスク対応計画の状況
f) 継続的改善の機会

監査結果の活用

① PMSの有効性の改善
② 継続的改善の機会
③ 個人情報保護マネジメントシステムのあらゆる変更の必要性に関する決定
④ 必要となる経営資源

10.2 継続的改善

組織は，個人情報保護マネジメントシステムの適切性，妥当性及び有効性を継続的に改善しなければならない。



PMS/ISMS の有効性の定期的な見直し(案)

1. 基本方針及び目的、並びに管理策の定期的な見直し

① 内部監査の結果、個人情報保護/情報セキュリティの事件・事故、有効性の測定結果、提案及び利害関係者からのフィードバックを考慮に入れる。

② 定期的(毎年3月)に個人情報保護/情報セキュリティ基本方針及び目的、並びに管理策の見直しを行う。

2. マネジメントシステムの有効性の評価

個人情報保護/情報セキュリティのマネジメントシステムに関する有効性については、適切な時期にその評価を行なう。

3. 管理策の有効性の評価

適用を決定した管理策(ISMSの場合は適用宣言書)については、適切な時期にその評価を行なう。詳細については、「PMS有効性評価手順書」または「ISMS有効性測定手順書」に従う。

まとめ

1. 内部監査の準備と真の目的
2. マネジメントシステムの運用に関するリスク
3. 今年度の監査ポイント
4. 委託の場合の監査事項
5. 個人情報保護マネジメントはこう変わる

内部監査の準備と真の目的

1. 監査前の準備次第で、効果・効率は上がる

① 経営陣がマネジメントシステムの導入目的を明確にし、資源の注入に本気で取り組んでいる。

② 監査員が自組織のマネジメントシステムの概略を理解している。

③ 各監査員の監査活動の準備が十分である。

a. 監査計画の作成：目的、監査基準、日程・所要時間、
監査チームの役割分担、監査報告書の記載項目、フォローアップ事項

b. 作業文書の作成：チェックリスト及び監査サンプリング計画

c. 文書レビューの実施：被監査部門の文書、記録、これまでの監査報告書

2. 目的・目標への達成可能性を含めて監査すること

マネジメントシステムの運用に関するリスク

1. マネジメントシステムの運用に関するリスク
2. リーダシップの欠如
3. 計画の欠如
4. 支援（人員。資金、器材、時間）の不足
5. 運用の欠如
6. パフォーマンス評価の不足
7. 改善の欠如

今年度の監査ポイント

1. 改正個人情報保護法対応
   - □ 個人情報の特定が適切になされているか？
     - ✓ 個人情報と個人データの違いを復習させる
     - ✓ 匿名化情報の特定は追加されていますか？
     - ✓ 個人情報を提供した・提供された際の記録
2. リスクマネジメント
   - □ 安全管理だけでなく、個人情報保護のリスクの特定の追加
     - ✓ **個人情報保護リスク**（個人情報の漏えい、滅失又はき損、関連する法令、国の指針その他規範への違反、経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれ）
3. 安全管理のマネジメントのポイント
   - □ クラウドシステムとオンプレミスシステムの確認
     - ✓ 依拠すべきガイドラインの確認
   - □ BYODの管理 → ルール通りの運用の徹底
   - □ 委託先への監査の実践（各部門1件づつでも）
4. （特定の部署：通常は事務局）
   - □ 苦情・事件・事故の届け出先の変更
5. 緊急事態対応の確認・徹底
   - □ 各部門単独ででも、できれば、訓練の実施

委託の場合の監査事項

1. 外部委託の部門管理責任者
2. 発注、進捗管理 、検収
3. 委託先の評価
4. 委託目的の明確化
5. 「個人情報登録申請／承認書」の作成と回議
6. 委託に係る個人情報の取得：同意の取得
7. 委託する場合の実施事項
   - ① 委託先の選定・評価
   - ② 委託先との契約条項の留意事項
   - ③ 委託先からの報告事項
8. 委託先に対する監査
9. 委託目的の終了時の実施事項

個人情報保護マネジメントはこう変わる
―JISQ15001改正のポイント（特にJISQ15001本文との関わり）―

1. 個人情報保護マニュアルの登場

→ マネジメント部分の独立へ

2. 有効性の評価の考え方の追加

✔ 当初管理策

→「安全管理＋個人情報保護対応」への残存リスクの有効性対応

✔ 年次の目的・目標管理

→ 個人情報保護目的の新設

✔ 監査・事件対応の有効性

3. リスクマネジメントの考え方

→ リスク分析・リスク対応

4. 是正処置・予防処置

→ 予防処置を廃して、他部署での処置はマネジメントで対応

（上級者編END）

株式会社エム・ピ・オー
代表取締役　森口修逸

URL:　www.m-p-o.co.jp
Email:　info@m-p-o.co.jp
TEL:　045-517-3246（MPO都筑オフィス）