

株式会社 ○○ 御中

**ISMS認証取得支援コンサルティング
のご提案**

特定非営利活動法人 東京ITコーディネータ

企業の社会的な責任の遂行とリスク対応

(CSR: Corporate Social Responsibility)

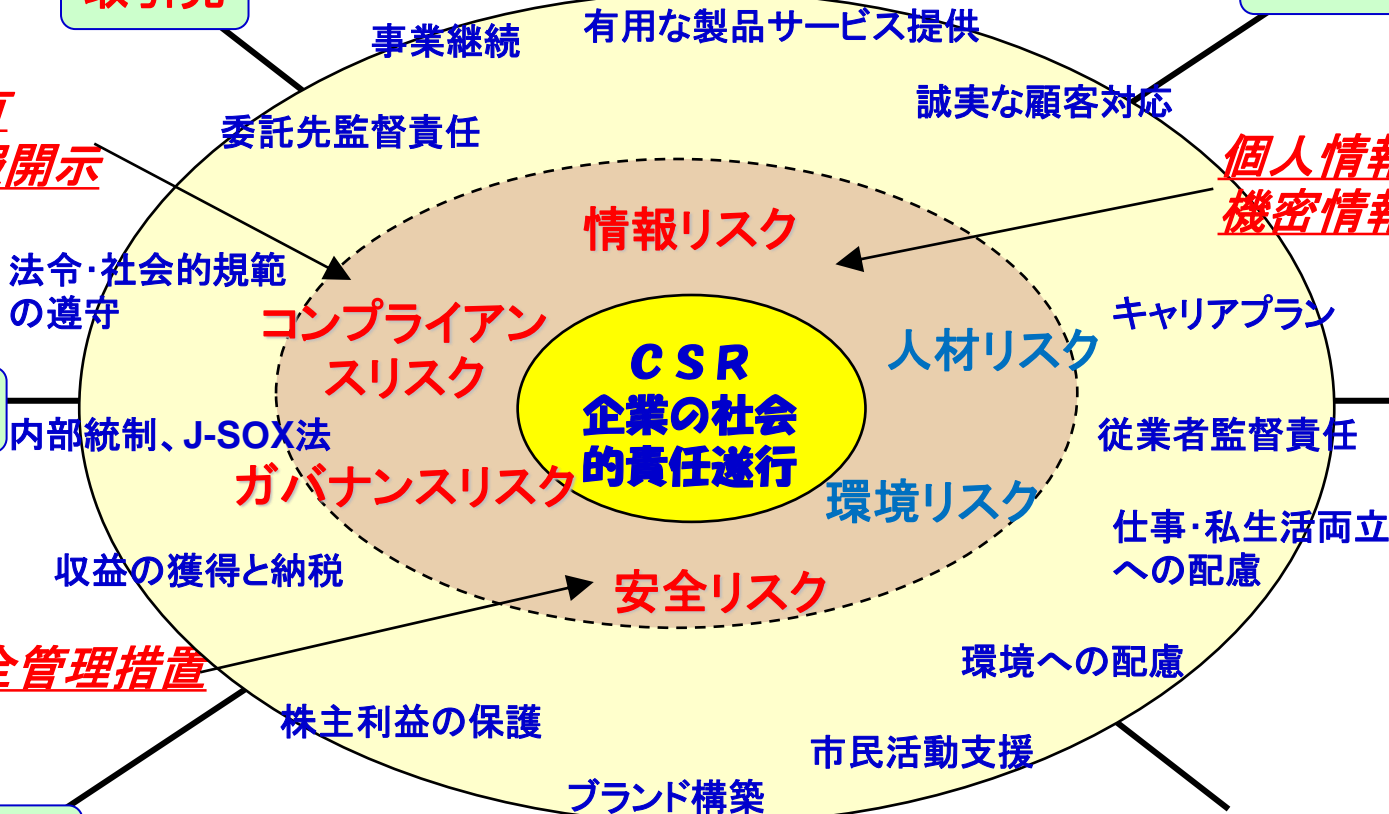
ステークホルダーとの関わりの中での活動

取引先

顧客

情報の共有
適切な情報開示

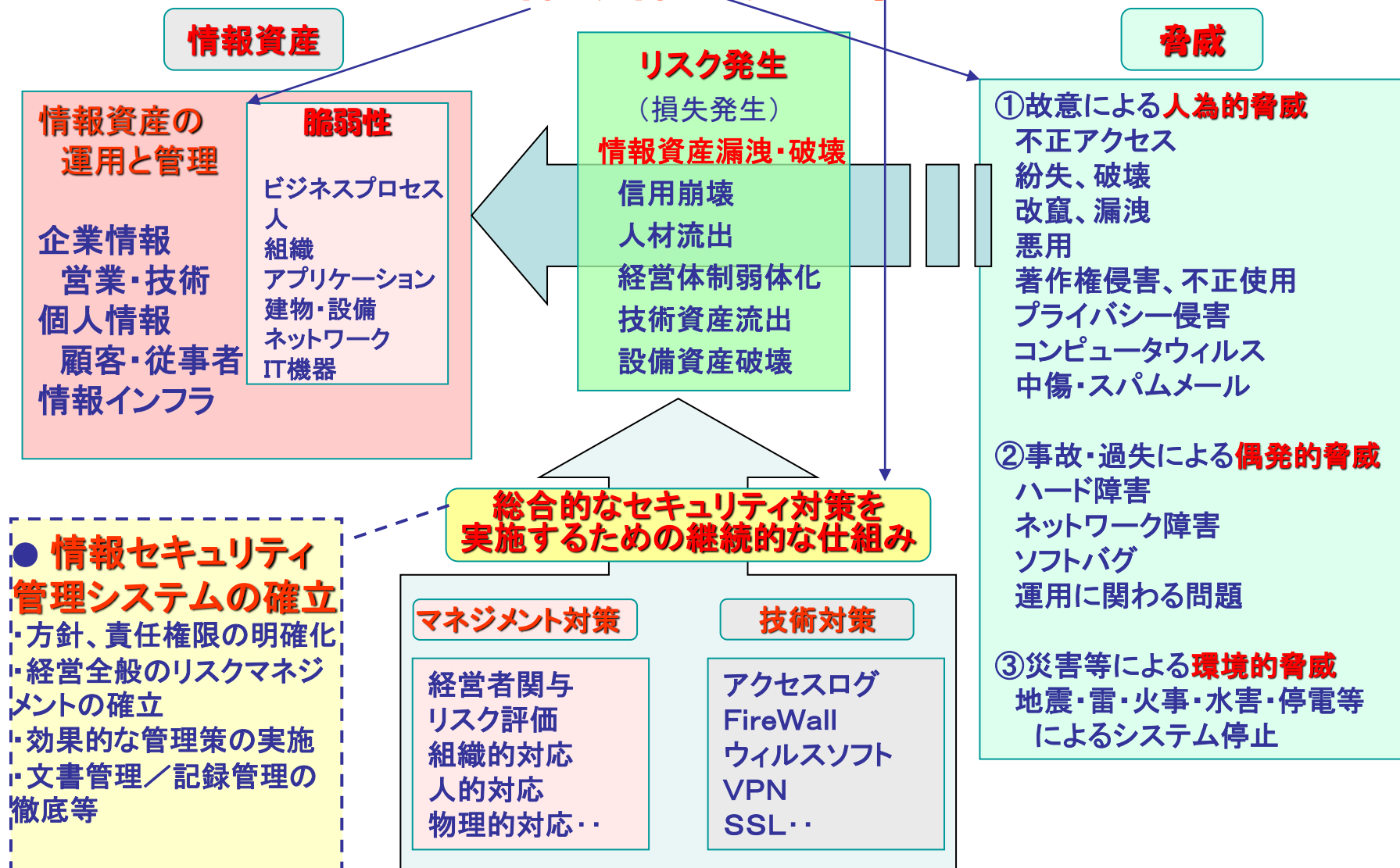
個人情報漏洩防止
機密情報流出防止



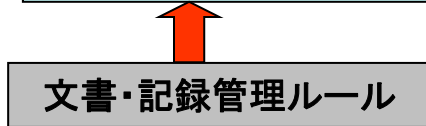
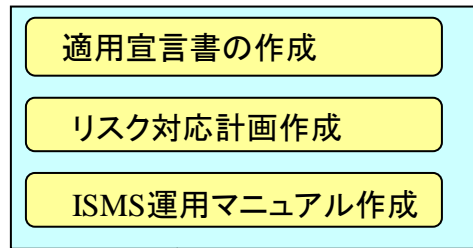
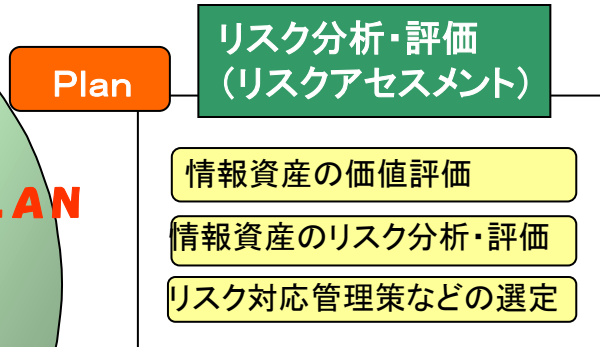
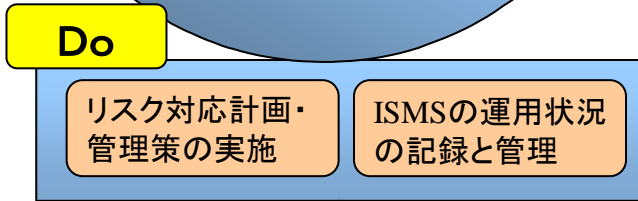
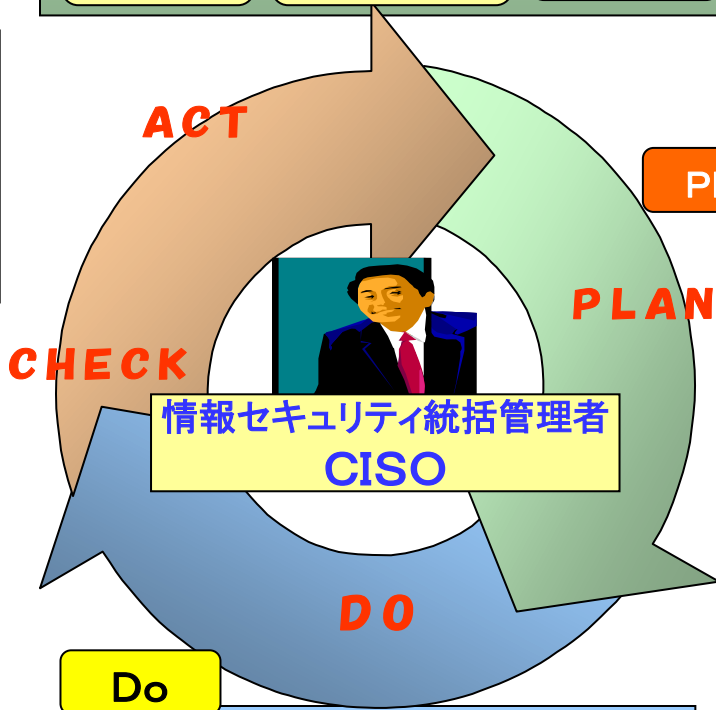
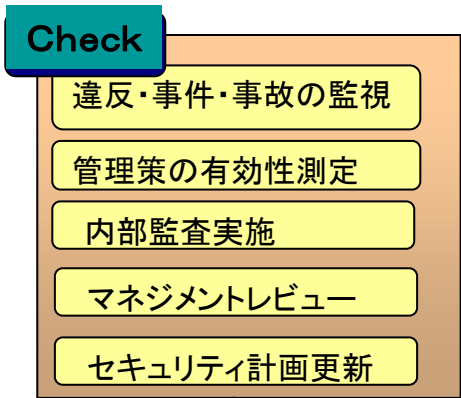
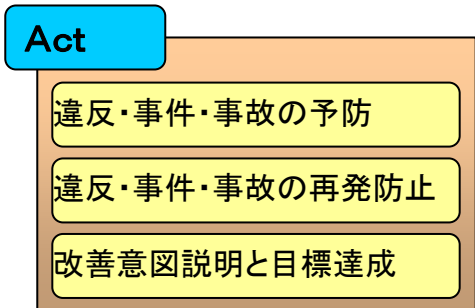
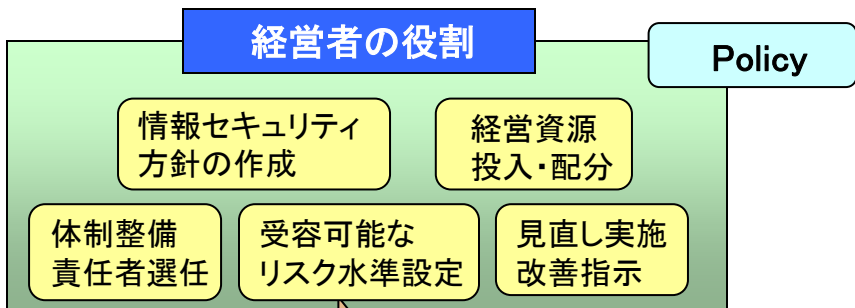
「企業価値」の向上

情報セキュリティ・リスクへの体系的対応

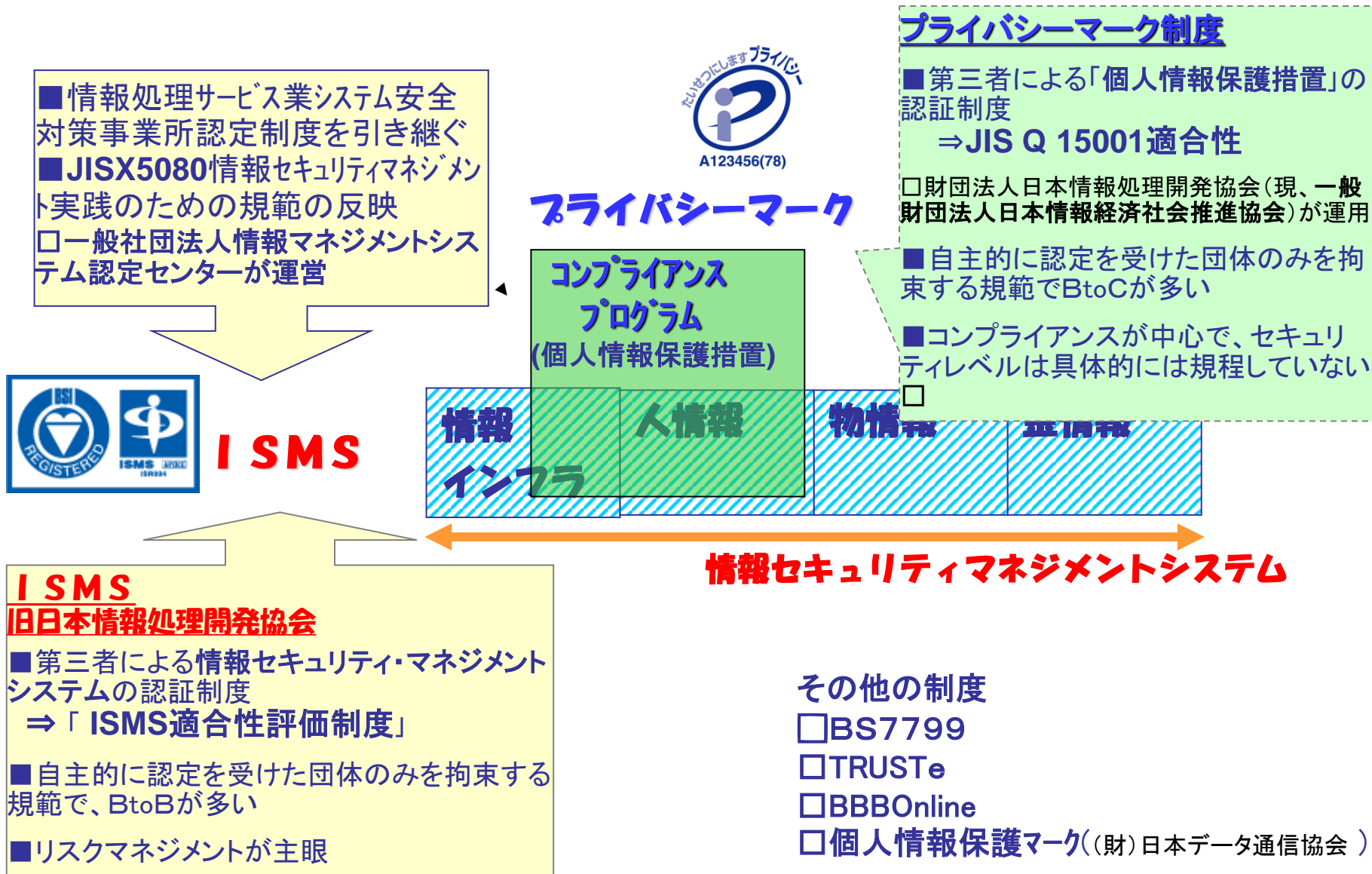
何を、何から、どう守るか？



ISMSが求めていること



「プライバシーマーク制度」と「ISMS適合性評価制度」との関係



「ISMS適合性評価制度」とは何か



1. ISMSの目的

ISMS適合性評価制度は、国際的に整合性のとれた情報セキュリティマネジメントとしての第三者適合性評価制度であり、本制度は、わが国の情報セキュリティ全体の向上に貢献するとともに、諸外国からも信頼を得られる情報セキュリティレベルを達成することを目的としたものです。

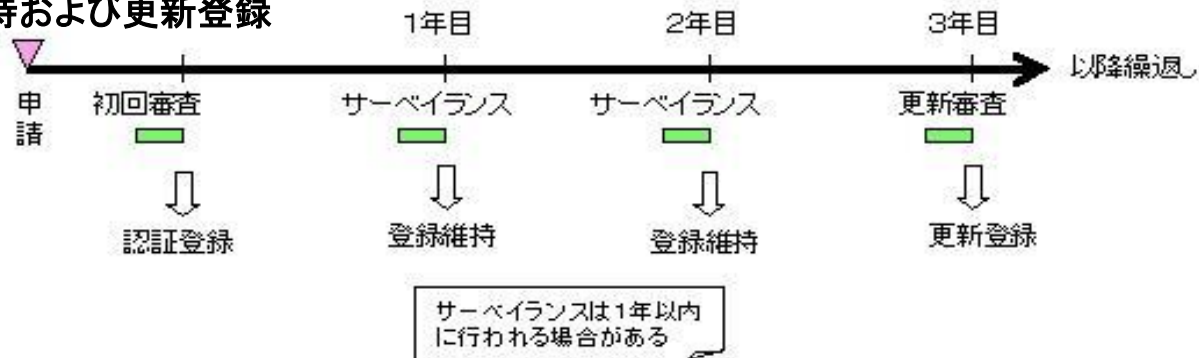
2. ISMSの認証基準

従来のISMSの認証基準(Ver. 2)は、英国規格BS 7799-2:2002に基づき作成したもので、本基準で使用する用語、表現については、JIS X 5080:2002(国際規格ISO/IEC 17799:2000)との互換性を確保していました。2005年のISO/IEC27001の発行に伴い、これに対応して国内規格のJIS Q 27001が発行され、ISMS認証基準(Ver. 2)は、2006年5月20日より「JIS Q 27001:2006」へ移行しました。

3. ISMSの適用範囲

ISMSの適用範囲は、企業情報を大量にマネジメントする企業内の部署を限定して導入を図ることが可能です。このため、ISMSはPマークに比べ大企業や事業所の多い企業に向いています。

4. 登録と維持および更新登録



ISMSの標準構築プロセス

ISO27001ベース(改1)

ISMS確立フェーズ 2~3ヶ月

ISMS導入・運用フェーズ 1~2ヶ月

ISMS監視・見直しフェーズ 1~2ヶ月

ISMS維持・改善 フェーズ2~3ヶ月

[P]

[D]

[C]

[A]

PJ準備

トップの関与

審査登録
機関決定

- ① 適用範囲境界定義
- ② ISMS基本方針策定
- ③ リスクアセスメント方針策定
- ④ リスクの識別
- ⑤ リスクの分析評価
- ⑥ リスク対応選択肢評価
- ⑦ リスク対応管理策選択
- ⑧ 残留リスク等の承認
- ⑨ 導入運用の経営陣の許可
- ⑩ 適用宣言書の作成

- ① リスク対応計画策定
- ② リスク対応計画の実施
- ③ 管理目的・管理策の実施
- ④ 有効性測定方法規定
- ⑤ 教育訓練の実施
- ⑥ 運用状況の管理
- ⑦ 経営資源の管理
- ⑧ セキュリティ事件事故対応

- ① 監視手順確立と実施
- ② ISMSの有効性見直し
- ③ 管理策の有効性測定
- ④ 残留リスク等の見直し
- ⑤ ISMS内部監査の実施
- ⑥ マネジメントレビュー実施
- ⑦ セキュリティ計画更新
- ⑧ ISMS実施状況の記録

- ① ISMS改善策実施
- ② 是正・予防処置の実施
- ③ 実施処置の伝達・合意
- ④ 改善目標の達成

維持審査
更新審査

スタート

現状の情報資産・HW/SWなど

成果物例

- ① 適用範囲定義書
- ② 情報セキュリティ基本方針
・情報セキュリティ基本規程
- ④ 情報資産目録(台帳)
- ⑤ リスク評価シート
- ⑥ リスクアセスメント報告書
- ⑦ リスク対応シート
・情報セキュリティ対策規程
- ⑧ 残留リスク一覧
- ⑩ 適用宣言書

手順書例

- ・情報資産管理手順書
- ・リスクマネジメント手順書
- ・情報セキュリティ対策基準

- ① リスク対応計画書
・情報セキュリティ運営体制案
・事業継続計画書
- ⑤ 情報セキュリティ教育・訓練計画書
・情報セキュリティ教育・訓練報告書
- ⑥ 情報セキュリティ運用状況報告書
- ⑧ 情報セキュリティ事件・事故報告書

- ・情報セキュリティ教育・訓練手順書
- ・ISMS文書管理手順書
- ・その他手順書

- ⑤ 内部監査計画書
・内部監査実施報告書
- ⑥ マネジメントレビュー議事録
- ⑦ セキュリティ計画改訂版
- ⑧ ISMS実施報告書

- ・内部監査手順書
- ・内部監査チェックリスト
- ・運営委員会実施手順

予備審査

登録審査

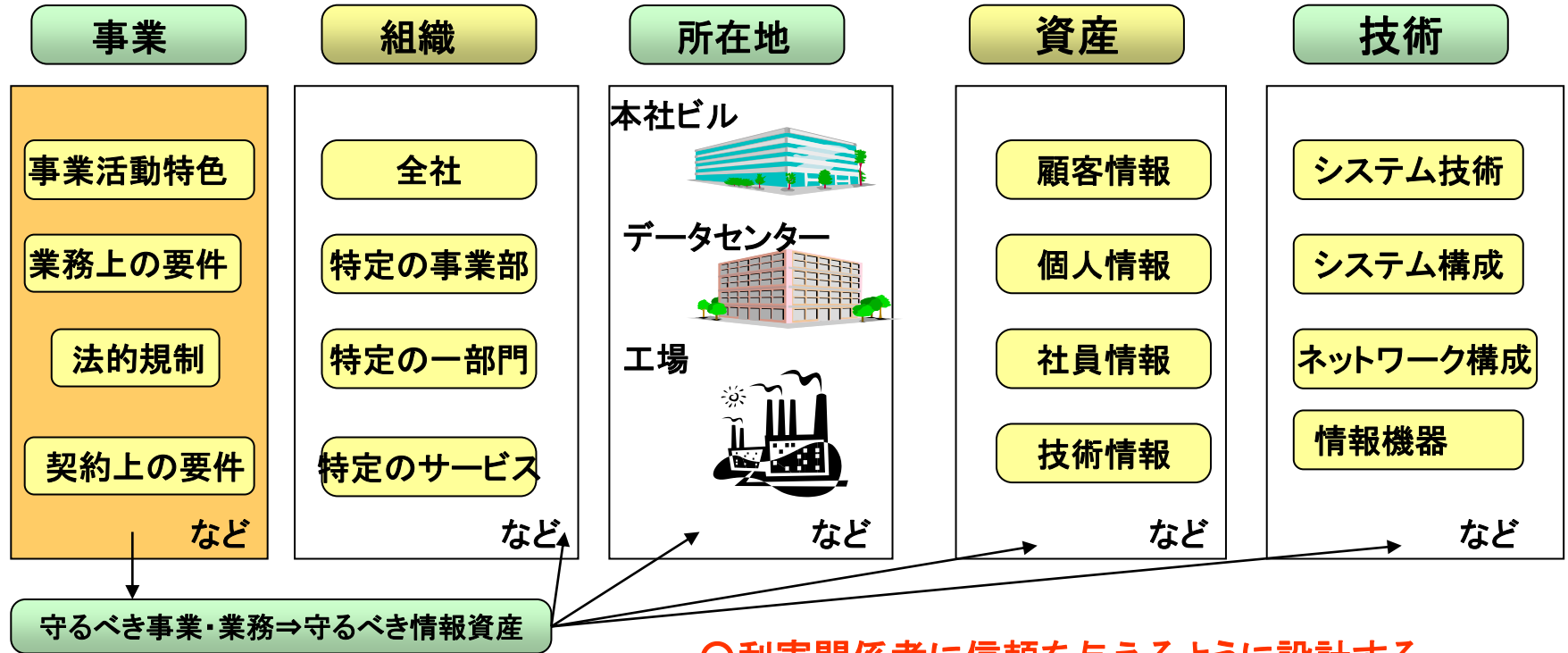
認証取得

- ① 改善計画/実施報告書
- ② 是正・予防処置報告書

作業スケジュール例

作業項目	PJ準備フェーズ	ISMS確立フェーズ			導入運用			監視・見直し		維持改善フェーズ		回数
		1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	
【I】準備フェーズ												1
①概略ヒヤリングと全体計画作成	○											
②ISMS導入プロジェクトの編成	○											
③PJキックオフ&情報セキュリティセミナー	○											
【P】ISMS確立フェーズ												11
①適用範囲定義		○										
②ISMS基本方針策定		○										
③リスクアセスメント方針策定		○										
④リスクの識別		←→										
⑤リスクの分析評価		←→										
⑥リスク対策選択肢評価		←→										
⑦リスク対応管理策選択・手順書作成		←→										
⑧残留リスク等の承認												
⑨ISMS導入運用の経営陣の許可				○								
⑩適用宣言書の作成				○								
【D】ISMS導入・運用フェーズ												3
①リスク対応計画策定					○							
②リスク対応計画の実施					←→							
③管理目的・管理策の実施					←→							
④有効性測定方法の規定					○							
⑤教育訓練の実施					←→							
⑥運用状況の管理					←→							
⑦経営資源の管理					←→							
⑧セキュリティ事件・事故対応					←→							
【C】ISMS監視・見直しフェーズ												3
①監視手順確立と実施							○					
②ISMSの有効性見直し							←→					
③管理策の有効性測定							←→					
④残留リスク等の見直し							○					
⑤ISMS内部監査の実施							○					
⑥マネジメントレビューの実施							○					
⑦セキュリティ計画更新							○					
⑧ISMS実施状況の記録							○					
【A】ISMS維持・改善フェーズ												2
①ISMS改善策実施										←→		
②是正予防措置の実施										←→		
③実施処置の伝達										○		
④改善目標の達成										○		
申請								★				
予備審査									★			
本審査										★	★	
ISMS認証取得												★

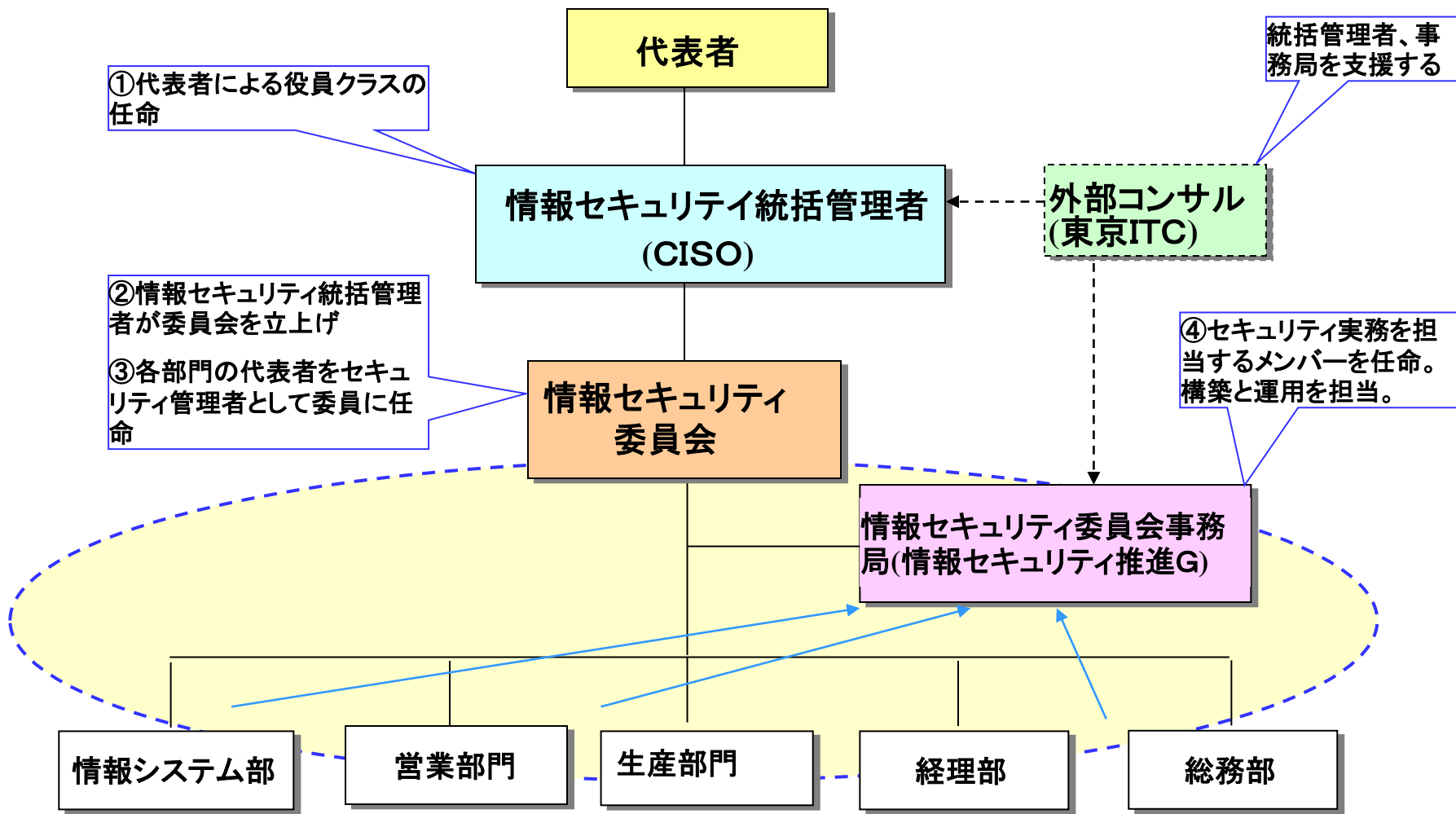
適用範囲の決定の考え方



5つの要素を切り口に適用範囲を決める

取得目的、取得目標、取得期間、取得体制

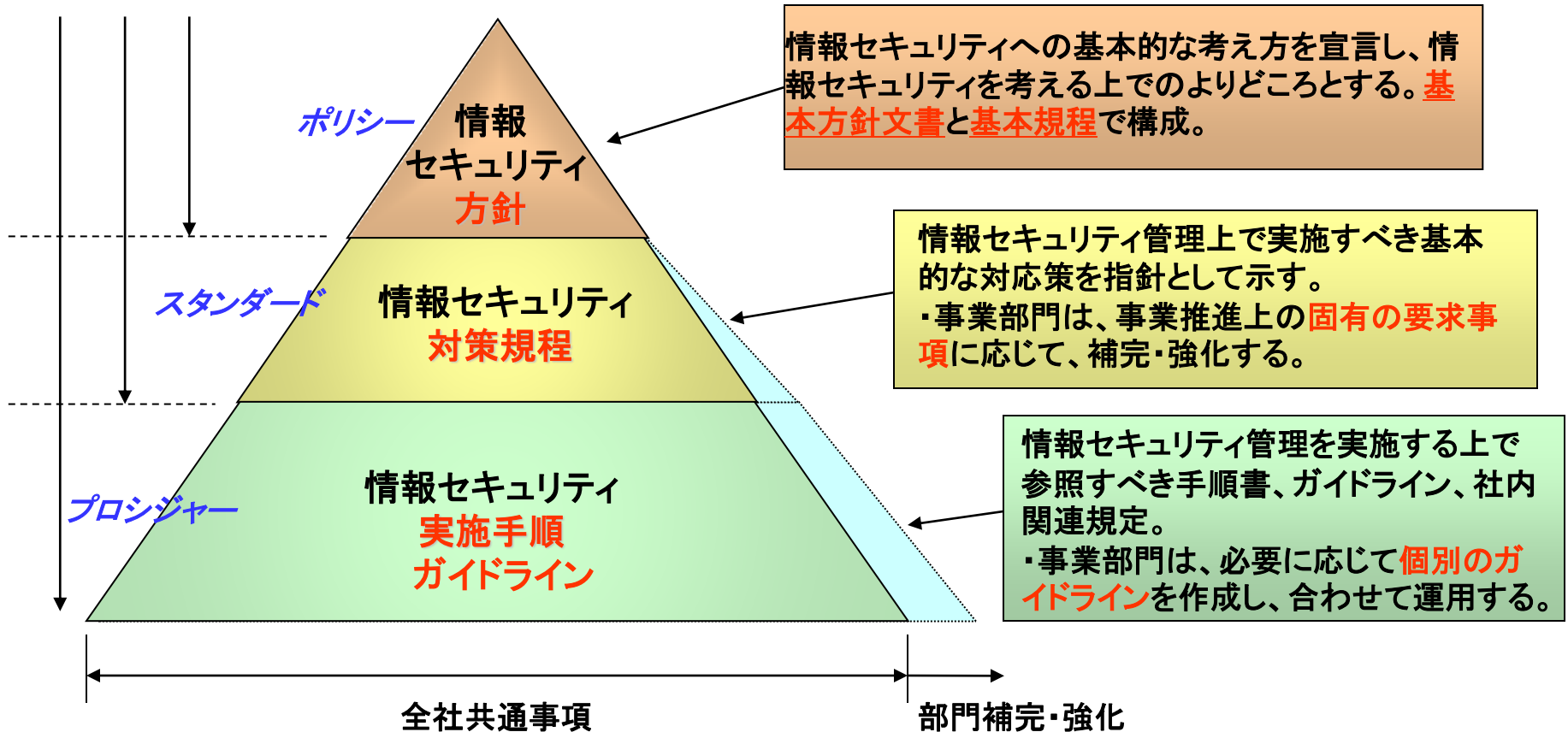
情報セキュリティ管理システム構築の推進体制(例)



情報セキュリティ文書体系

・「情報セキュリティ」とは情報の機密性、完全性、可用性を保つことであり、このセキュリティに対する考え方(ポリシー)を明文化し、全社員で共有する

「セキュリティポリシー」



ISMS文書体系

	ISMS文書	実施記録等	関連規程・マニュアルにおけるセキュリティ関連事項	実施記録
ポリシー	<div style="border: 1px dashed black; padding: 5px;"> 情報セキュリティ方針 </div>	ISMS構築稟議書 ISMS構築社内通達		
	情報セキュリティ基本方針 情報セキュリティ基本規程 基本方針文書規程	情報セキュリティ方針書 ISMS適用範囲規程書 ISMS適用宣言書	<div style="border: 1px dashed gray; padding: 5px;"> 情報システム構築規程 情報システム取得・開発規程 物理・環境のセキュリティ管理規程 外部サービス規程 </div>	各種申請書 入退出管理記録 契約書・SLA
スタンダード	情報セキュリティ対策規程	リスク対応計画書 管理策別目標・有効性評価表	<div style="border: 1px dashed gray; padding: 5px;"> 情報システム運用規程 基幹システム運用規程 利用者ID管理基準 ユーザ認証基準 ウィルス対策基準 バックアップ基準 暗号化管理規程 </div>	情報システム運用記録 アクセスログ 利用者ID申請書 特権パスワード管理台帳 バックアップ記録
	情報セキュリティ委員会規程 マネジメントレビュー規程	委員辞令 委員会議事録 レビュー議事録		
	セキュリティ事象対応規程 緊急時・異常時対応規程	セキュリティ事象事故報告書	<div style="border: 1px dashed gray; padding: 5px;"> 情報システム利用規程 情報資産調達規程 基幹システム利用規程 OAシステム利用規程 グループウェア等利用規程 安全管理規程 </div>	情報資産購入申請書 基幹システム利用申請書 グループウェア等利用申請書
	事業継続計画規程			
	適用法令規程		<div style="border: 1px dashed gray; padding: 5px;"> 情報システム維持規程 変更管理規程 情報システム保守規程 </div>	保守報告書
	ISMS教育規程	教育計画書 教育実施報告書	<div style="border: 1px dashed gray; padding: 5px;"> ネットワーク管理規程 社内ネットワーク管理規程 外部ネットワーク利用規程 </div>	ネットワーク監視報告書
	ISMS内部監査規程	監査計画書 監査実施報告書 是正処置報告書		
	ISMS文書・記録管理規程	規程文書一覧 記録帳票一覧		
	<div style="border: 1px dashed black; padding: 5px;"> 情報セキュリティ対策実施手順 </div>		<div style="border: 1px dashed gray; padding: 5px;"> 業務関連規程 就業規則 罰則規程 人的セキュリティ対策規程 </div>	誓約書(社員) 誓約書(外部)
プロシジャー	情報資産管理手順書	情報資産調査票/台帳 情報資産目録	<div style="border: 1px dashed gray; padding: 5px;"> 職務規程 各種業務マニュアル </div>	職務定義書 各種手順書
	リスクマネジメント手順書	リスク管理票 残留リスク一覧	<div style="border: 1px dashed gray; padding: 5px;"> 外注・購買管理規程 個別業務別マニュアル </div>	外部委託契約書 秘密保持契約書
			<div style="border: 1px dashed gray; padding: 5px;"> 個人情報保護関連規程 各種規程・細則 </div>	
			その他社内規定	社内稟議規程 稟議書

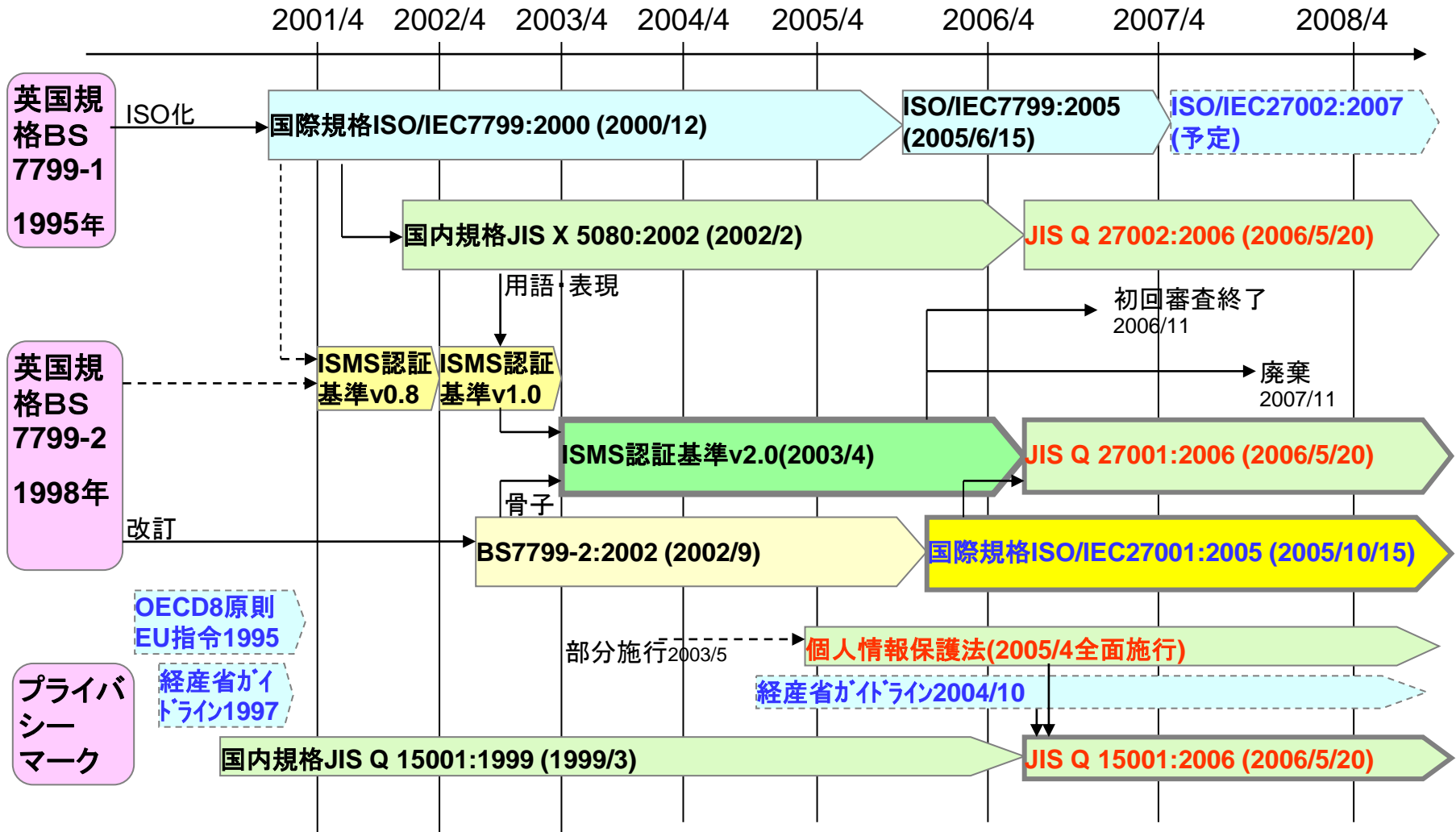
PマークとISMSとの比較（1）

	プライバシーマーク	ISMS
目的・狙い	<ul style="list-style-type: none"> ・「個人情報」の取扱について適切に扱っている事業者を認定する。 ・個人の権利・利益を守る。 	<ul style="list-style-type: none"> ・企業の情報資産全般のセキュリティマネジメントシステムの確立と運用・維持できていることを認定する。 ・情報資産をリスクから守る。
適用対象	<ul style="list-style-type: none"> ・自ら保有する「個人情報」 ⇒個人情報がある程度保有する業種・事業者向け ・認定申請に当たっては事業者単位の取り組みが前提となっている 	<ul style="list-style-type: none"> ・ソフト、ハードを含む「情報資産全般」 ⇒業種に関係なく適用 ・組織の必要性に合わせて、部門・場所等の適用範囲を合理的に決定して申請できる
審査適用規格	JIS Q 15001 個人情報保護マネジメントシステム－要求事項	ISO/IEC27001:2005 / JIS Q 27001
認証取得状況	<ul style="list-style-type: none"> ・1998年スタート ・2020.4現在・・・16,459事業者 	<ul style="list-style-type: none"> ・2002年スタート ・2020.4現在・・・6130事業者
認証取得方法	・事業者単位(全社単位)に取得	・適用範囲を限定し逐次範囲拡大可能
維持更新	・2年に1回更新	<ul style="list-style-type: none"> ・毎年サーベランスがある ・3年に1回更新

PマークとISMSとの比較（2）

	プライバシーマーク	ISMS
申請費用	申請費用は中規模企業の場合600千円、更新料は450千円(2年毎)	従業員数、拠点数、機関によるので見積り要例:1拠点10名で申請時1290千円、毎年263千円。3拠点60名で申請時1720千円、毎年437千円、更新時787千円(3年毎)。
管理の対象範囲	<ul style="list-style-type: none"> ・個人情報保護は、個人情報の安全管理策を実施するだけでなく、個人情報の本人の権利に対応することも含まれる。 ・情報取得時には事前に利用目的等を伝えた上で本人の同意をとることが必要であり、取得後も本人からの修正・削除などの要望に応じる必要がある。 	<ul style="list-style-type: none"> ・基本的に、組織の事業活動全般及びリスク全般を考慮し、事業上の要求事項、法的又は規制要求事項に対するリスクアセスメントによりセキュリティ対策(管理策)を実施する。
マネジメントシステム構築	<ul style="list-style-type: none"> ・個人情報の安全管理策を構築することに加えて、情報主体の権利に対する要求への管理策が必要となる。また、個人が対象となるために、苦情処理窓口を準備して対応するなど消費者保護の側面を考慮する必要がある。 	<ul style="list-style-type: none"> ・組織の事業継続や、運用コストも配慮した総合的な観点でセキュリティ対策の取組みがされているかが重要なポイントとなる。
特色	<ul style="list-style-type: none"> ・日本固有の制度 ・個人情報が多い企業で有効 ・管理策を決定する手順は明確でない ・B2Cビジネスに有効 	<ul style="list-style-type: none"> ・ISOに準拠したグローバルスタンダード ・情報の安全を守る管理策を決定する手順が明確 ・主としてB2Bビジネスに有効

情報セキュリティの規格変革期



NPO法人「東京ITC」が提案する取得支援作業

お客様の「顧客満足度向上マネジメント」と
「コンプライアンス経営の確立」を支援

