

情報セキュリティ対策に関連する
基準・ガイドラインの現状・課題について

ASP・SaaSの情報セキュリティ対策に関する研究会
事務局

2007年8月8日

目次

	<u>ページ</u>
●本研究会で議論の対象とする既存の基準・ガイドライン(案)	2
●重点を置いて検討すべき情報セキュリティ等の分野	3
●情報セキュリティ等の各分野と既存の基準・ガイドラインとの対応関係の整理	4
●既存の基準・ガイドラインの普及状況	7
●既存の基準・ガイドラインの成果	9
●既存の基準・ガイドラインの陥りやすい問題点	10
参考資料	15

本研究会で議論の対象とする既存の基準・ガイドライン(案)

本研究会で議論の対象とするガイドラインを以下のように設定する。

条件

対象

1. 電気通信事業(ASP・SaaS事業者等)に関連する法令、基準、ガイドライン

- ・電気通信事業法
- ・電気通信事業における個人情報保護に関するガイドライン (総務省)
- ・情報通信ネットワーク安全・信頼性基準 (昭和62年郵政省告示第73号)
- ・プロバイダ責任制限法
- ・不正アクセス禁止法

2. マネジメントシステムの運用(PDCAサイクル)に関する法令、基準、ガイドライン

- ・BS7799 Part2 (ISO/IEC 27001:2005)
- ・MICTS
- ・JIS Q15001:2006
- ・ISO/IEC 20000-1:2005
- ・BS 25999

3. 対策の方針、基本ルール、及び具体的な事例(ベストプラクティス)を網羅した法令、基準、ガイドライン

- ・BS7799 Part1 (ISO/IEC 27002:2005)
 - ・FISC
 - ・NIST
 - ・ISO/IEC 20000-2:2005
 - ・PD0005、PD0015
 - ・ITIL
 - ・COBIT (IT Governance Institute)
 - ・金融機関等におけるコンティンジェンシープラン策定のための手引書
 - ・電子自治体 基幹系SLA設定例 (ASPIC Japan)
 - ・公共ITにおけるアウトソーシングに関するガイドライン(2003年 総務省)
 - ・電気通信事業における情報セキュリティマネジメント指針(2006年 総務省)
- (注)電気通信事業法が義務付ける要求事項に対応した目的、管理策等を含む

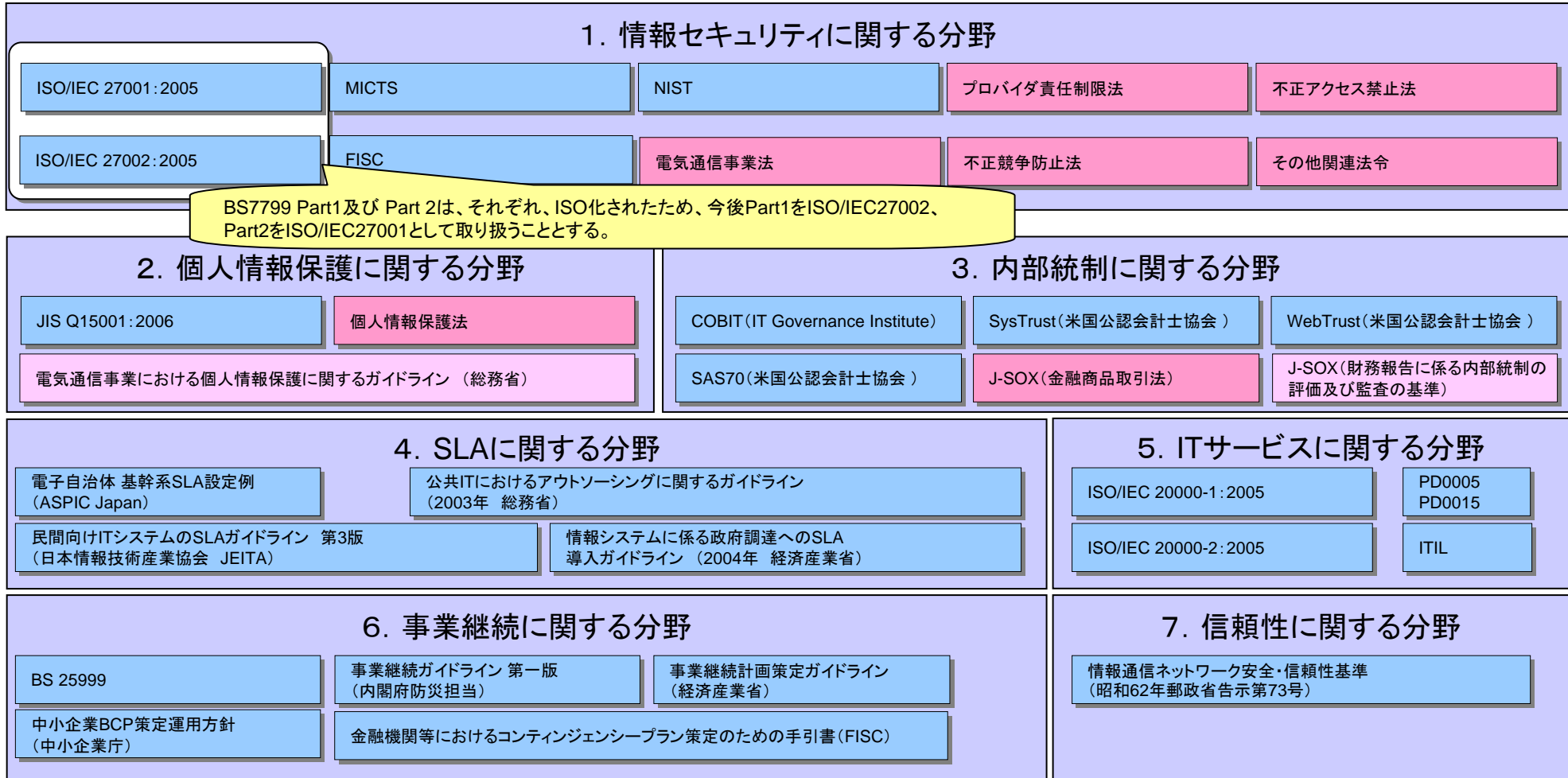
●重点を置いて検討すべき情報セキュリティ等の分野

重点を置いて検討すべき情報セキュリティの分野を以下の7分野に設定する。

1. 情報セキュリティに関する分野（BS7799をベースとする）
2. 個人情報保護に関する分野
3. 日本版SOX法に関する分野
4. SLAに関する分野
5. ITサービスマネジメントに関する分野
6. 事業継続に関する分野
7. 信頼性に関する分野

情報セキュリティ等の各分野と既存の基準・ガイドラインとの対応関係の整理 (1)

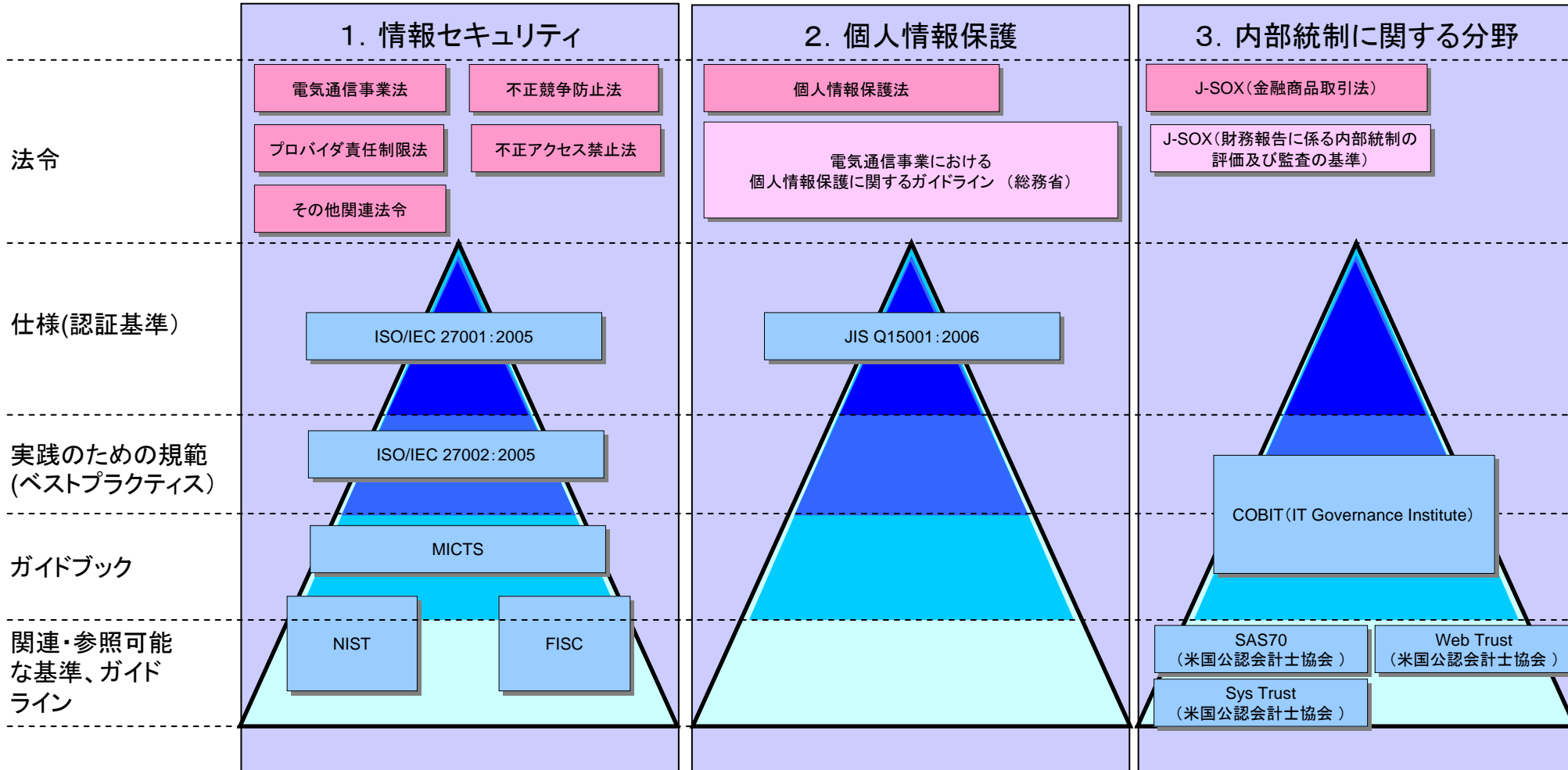
情報セキュリティ分野を中心に、以下の7つの関連分野について既存の基準・ガイドラインを抽出した。



凡例: 法令 省庁発行ガイドライン 基準・ガイドライン

情報セキュリティ等の各分野と既存の基準・ガイドラインとの対応関係の整理 (2)

情報セキュリティ、個人情報保護、内部統制の各分野において、前ページで抽出した法令、基準、ガイドラインの位置関係は以下の通り。



凡例:

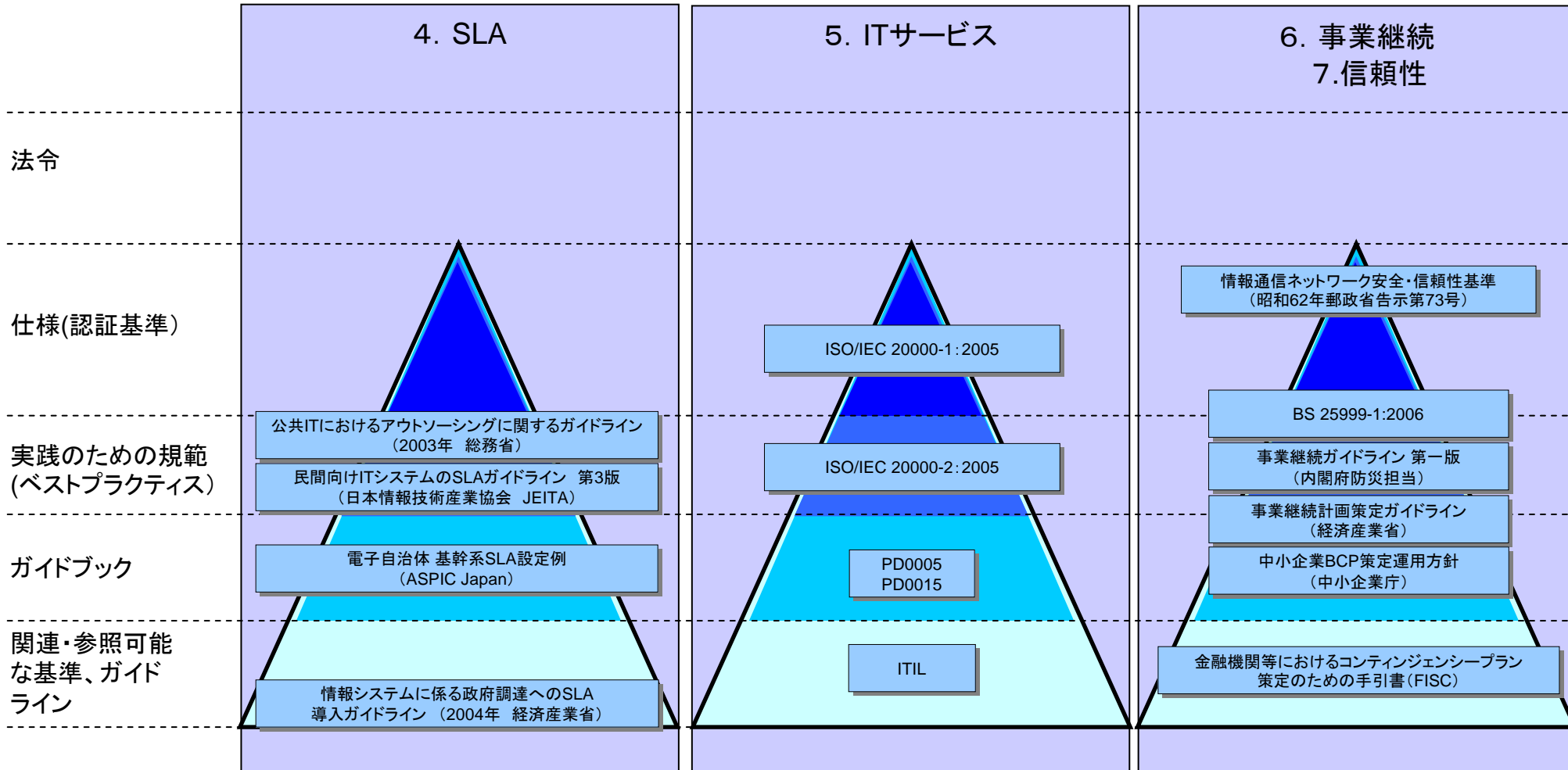
法令

省庁発行ガイドライン

基準・ガイドライン

情報セキュリティ等の各分野と既存の基準・ガイドラインとの対応関係の整理 (3)

SLA、ITサービス、事業継続性、信頼性の各分野において、前ページで抽出した法令、基準、ガイドラインの位置関係は以下の通り。



凡例:

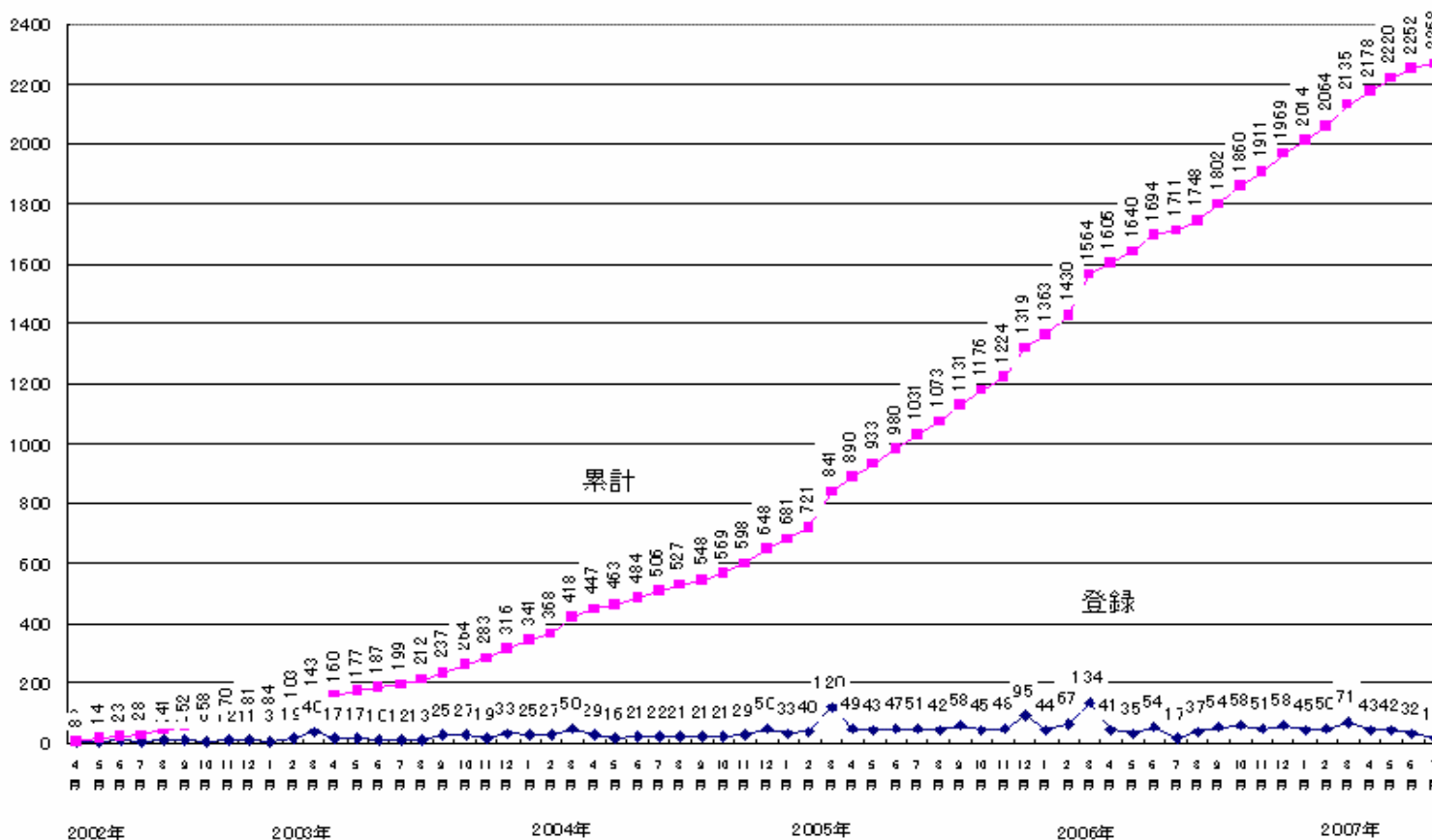
法令

省庁発行ガイドライン

基準・ガイドライン

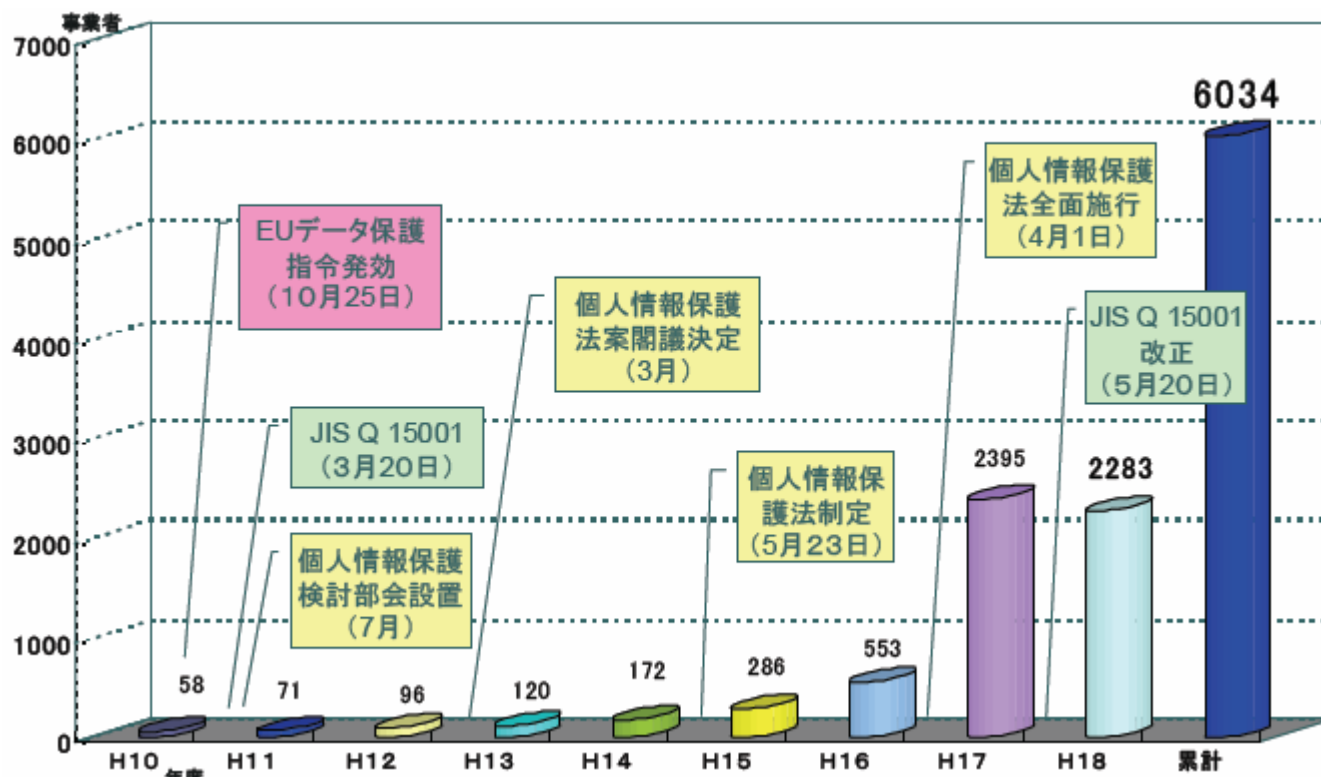
既存の基準・ガイドラインの普及状況 ① ISMS適合性評価制度

個人情報保護法の施行等により情報セキュリティに関する関心が高まる中、2004年から2005年度にかけて認証登録者数が大きく増加している。サービスや事業規模に合わせて取得できるため、全組織での取得のみならず、1つの部門での取得、複数組織が共同で取得、地方自治体等の公的機関による取得等の様々な取得ケースがあるのが特徴である。ISMS適合性評価制度が運用開始され5年を経過しているが、依然として右肩上がりの伸びを示している。



既存の基準・ガイドラインの普及状況 ② プライバシーマーク制度

個人情報保護法の施行により認定事業者数は急増している。2007年8月5日現在で、認定事業者数は延べ8,035社となっており、着実に増加している。ISMSでは比較的大規模な事業者による取得が目立つが、プライバシーマークは、中小規模の事業者の取得も多くなっている。

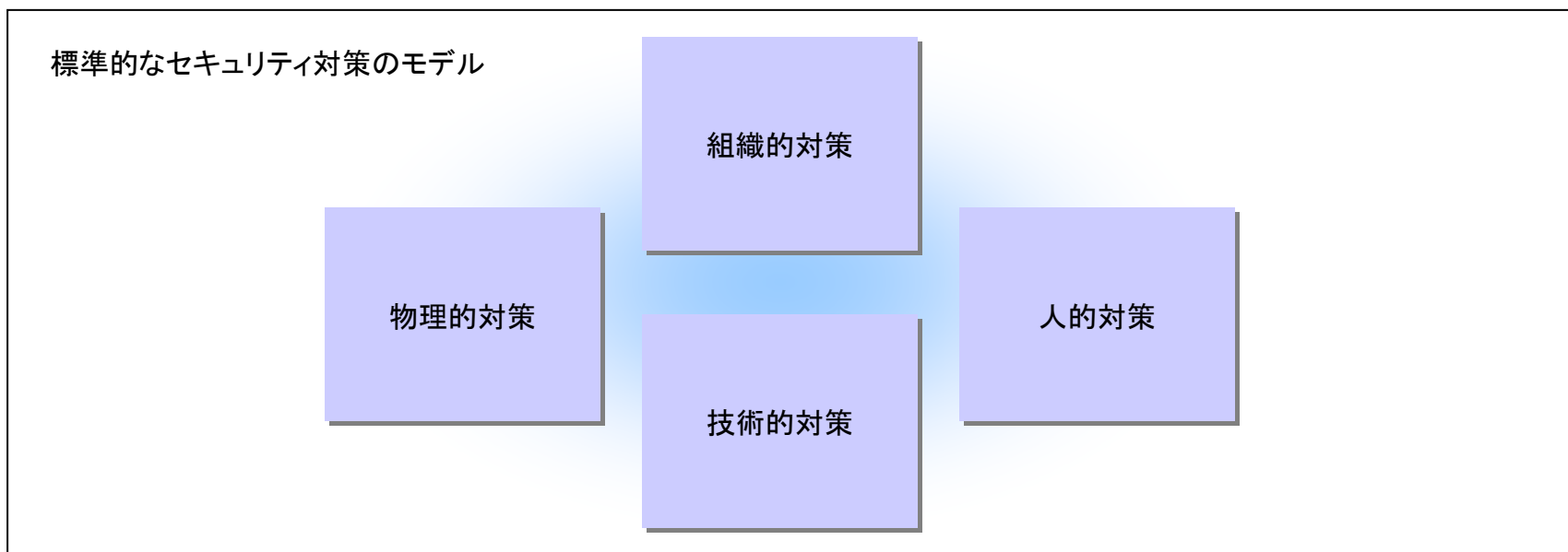


既存の基準・ガイドラインの成果

既存の基準・ガイドラインは、様々な業種業態に適用可能なベストプラクティスとしてのモデルを採用している。情報セキュリティに関するリスクに対して組織がとりうる合理的な対策を講じ、そのマネジメントシステムとしてのPDCAサイクルを回していく仕組みを提供するものである。これらの既存の基準・ガイドラインは、情報セキュリティの汎用的な基準として認証取得者のみならず多くの組織に採用されている。

例えば、組織が外部委託を行う際の選定基準や官公庁の入札要件として採用されるケースが増えてきている。また、個人情報保護法制定の際の個人情報の安全管理措置として各省庁が発行するガイドラインにもその考え方が反映されている。

既存の基準・ガイドラインは、情報セキュリティを考えていく上で業種・業態という枠組みを超えた共通言語を提供しているという意味で大きな成果であると考えられる。

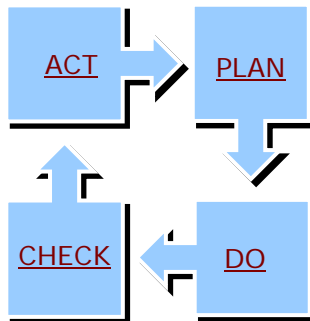


既存の基準・ガイドラインの陥りやすい問題点

既存の基準・ガイドラインは、様々な業種業態に適用可能なモデルを採用している。そのため運用方法が業種業態の特性によって異なるため効果的にセキュリティ運用を実装している組織とセキュリティを高めていく意識は持っているものの実際にはセキュリティ運用が適切でない組織とが同じレベルでの認証を受けている。従って、情報セキュリティの認証を取得しているからといって、セキュリティが十分であるとは言い切れないのが現状である。

既存の基準・ガイドラインの特長

- ・形態、規模及び事業の性質を問わず適用可能
- ・正当と判断できる理由があれば、自らがリスクの受容水準を決めることができる
- ・汎用的であるため、適用を支援するコンサルタントが豊富に存在する
- ・PDCAモデルに基づいたマネジメントシステムの枠組みを提供



基準・ガイドラインは情報セキュリティを確保するためのツールでしかない。構築や運用方法の自由度が高いため、その使い方を間違えると次のような課題に直面する場合がある

既存の基準・ガイドラインで陥りやすい問題

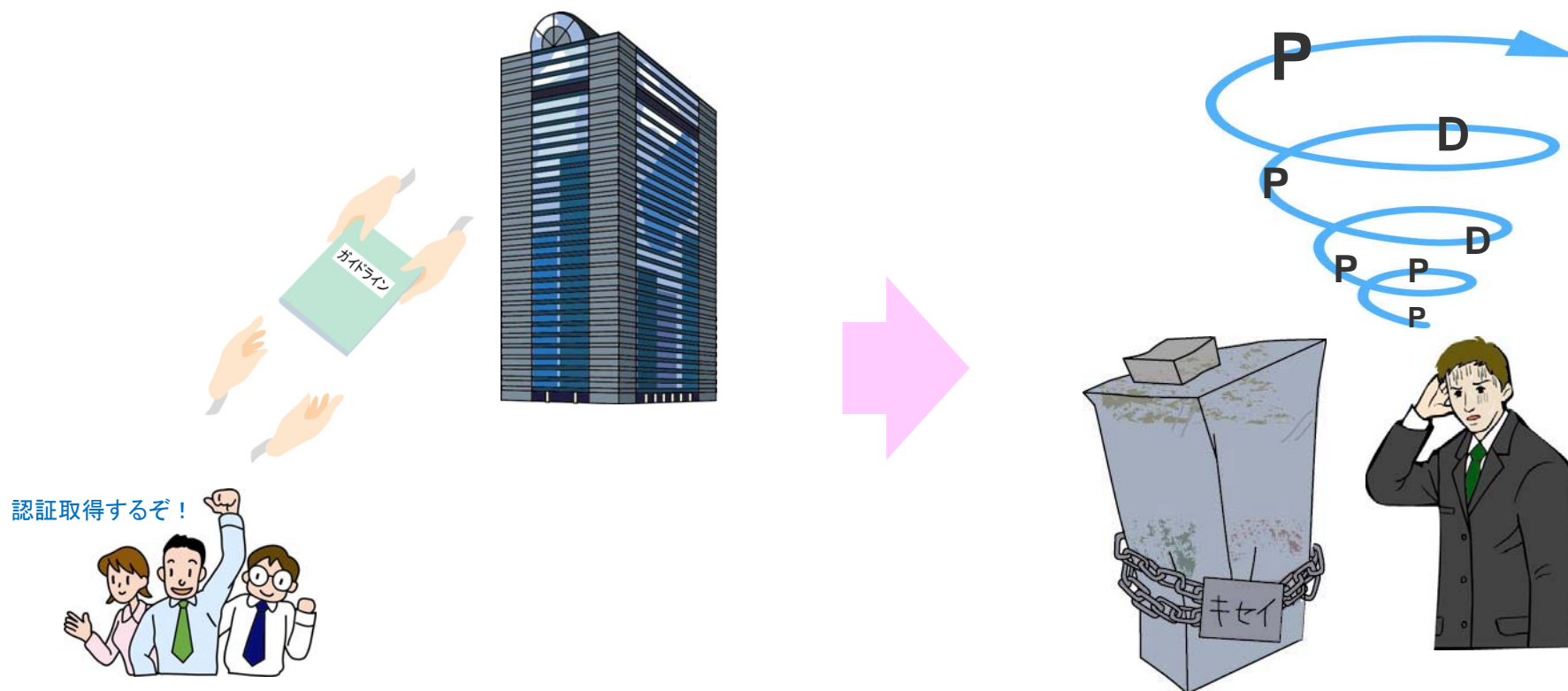
- ・どこまで対策すべきかの判断ができないため過剰な対策になる傾向がある
- ・リスクアセスメントの方法を誤ると、本来守るべき情報資産が対象にならない場合がある
- ・コンサルタントに大きく依存すると、不在時に運用が回らなくなる
- ・形式的に運用を行っているだけでも認証を継続できる場合がある（PDCA運用の形骸化）

● 既存の基準・ガイドラインの陥りやすい問題点 ケース①: 過剰セキュリティ対策

モデル例 ①

ASP・SaaS業界のA社は、設立2年目にして事業がようやく軌道に乗ってきました。社長は情報セキュリティに力を入れるべく知り合いの大手金融会社が利用している情報セキュリティのためのマネジメントシステムの雛形を借りてきました。

ところが、業種の異なる企業のガイドラインを適用したため、今回の場合は過剰対策となってしまうマネジメントは回らず大変なことに……



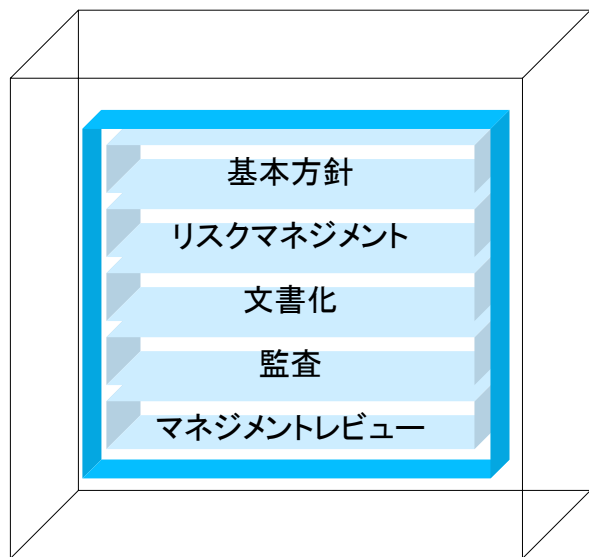
既存の基準・ガイドラインの陥りやすい問題点 ケース②:リスクが十分に対策されていない

モデル例 ②

ソフトウェア開発会社のB社は、情報セキュリティのマネジメントシステムを導入することにしました。開発業務に特に力を入れた基本方針を作成し、リスクマネジメント、文書化、監査、マネジメントレビューと順調に構築し、無事認証を取得することができました。

ところが、B社はソフトウェアの販売も行っているのですが、個人情報についての人的セキュリティ対策が不十分だったため、社員が顧客情報を容易に持ち出してしまい漏えい事故を起こしてしまいました。

どうやら、リスク分析がきちんとは行われていなかったようです。



認証取得



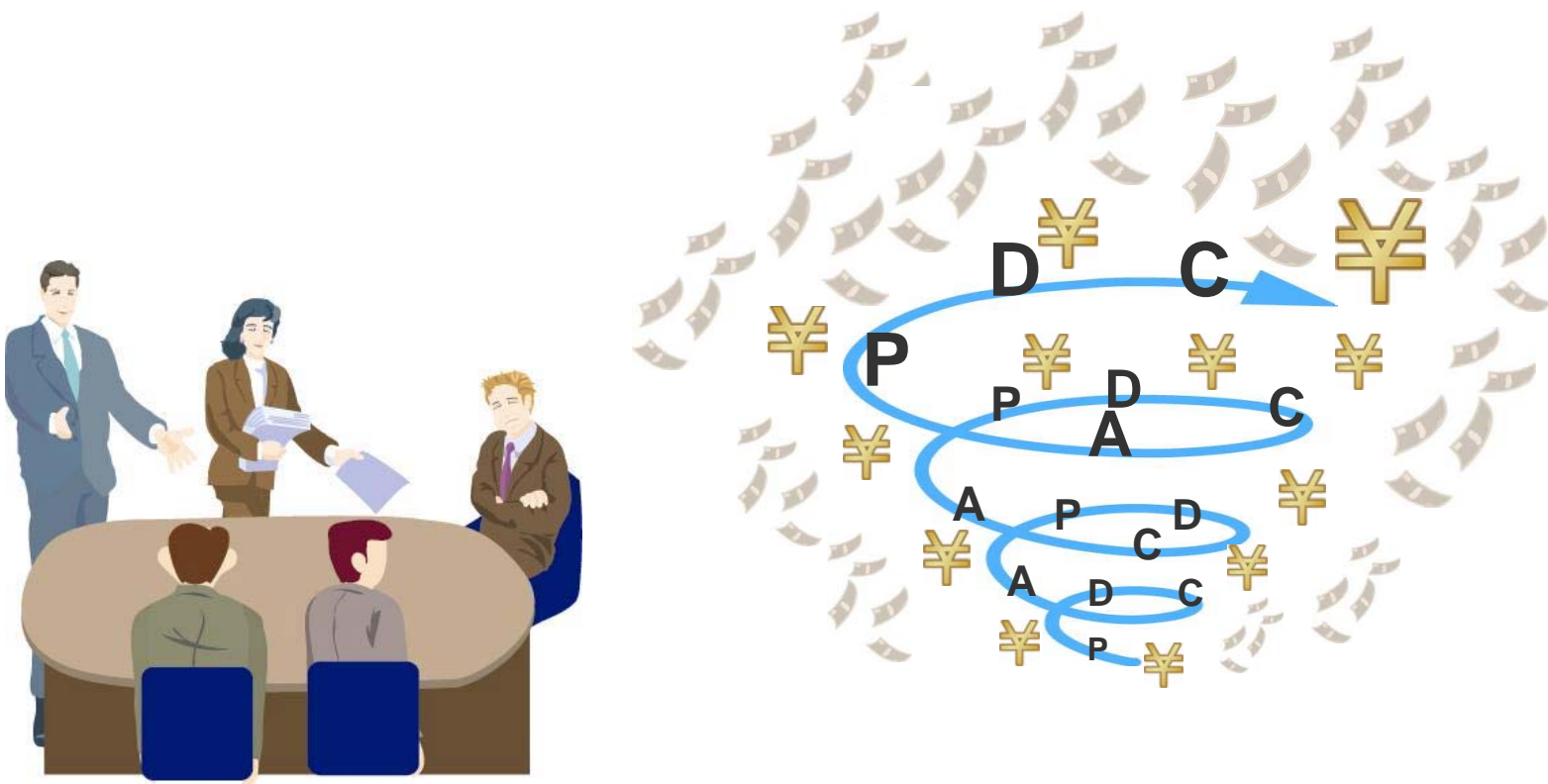
マネジメントシステムの枠組みは出来ていたが、中身が...

既存の基準・ガイドラインの陥りやすい問題点 ケース③: コンサルがないと回らない

モデル例 ③

大手ASP・SaaS会社のC社は、情報セキュリティのためのマネジメントシステムを導入することにしました。そこで情報セキュリティコンサル会社のD社にお願いし、忙しい社員の負担を減らすためコンサルタントを多く雇いました。コンサル費用は膨大になりましたが、大企業であり業績も良いのでお金でセキュリティを保てるのなら問題ありませんでした。

ところが、コンサルタントに任せきりにしているため、社員の知識はつかず、セキュリティ対策のために度々お金がかかります。お金のPDCAスパイラルを回す結果となってしまいました。



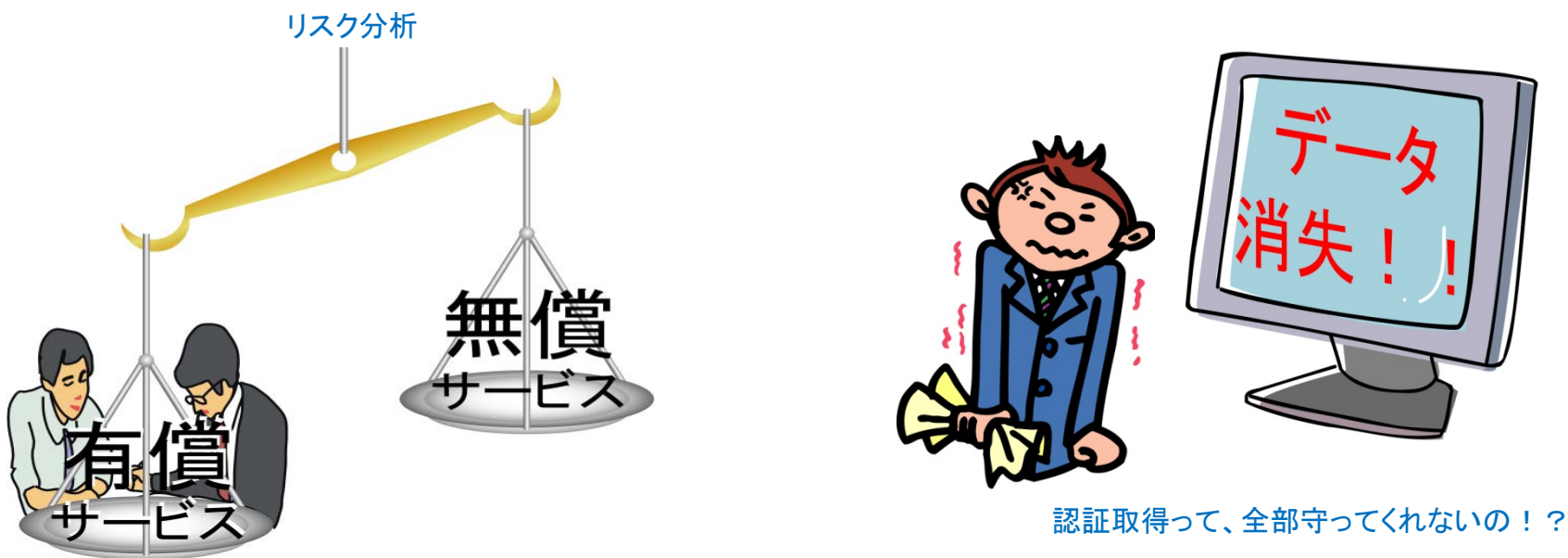
既存の基準・ガイドラインの陥りやすい問題点 ケース④:ユーザーから見ると内容が不透明


モデル例 ④

設立1年目のE社は、社員のスケジュールを管理するG社のASP型サービスを利用しています。まだまだ設備投資などに資金を多く費やすことができないため、G社の無償のサービスであるWEBメールを利用し、コストダウンを図っていました。情報セキュリティの面での心配もありましたがセキュリティに関する認証を取得していることがG社のホームページに記載されていたため、安心してクライアントとのメールのやりとりを行っていました。

ところが、G社の無償サービスのデータベースが一部消失する事故が起きてしまい、クライアントとの重要なやりとりのメールが6ヶ月分消えてしまう結果となってしまいました。

どうやら、G社は有償サービスをより重視したリスク分析を行っており、無償サービスのリスクは下げて構築していたようです。

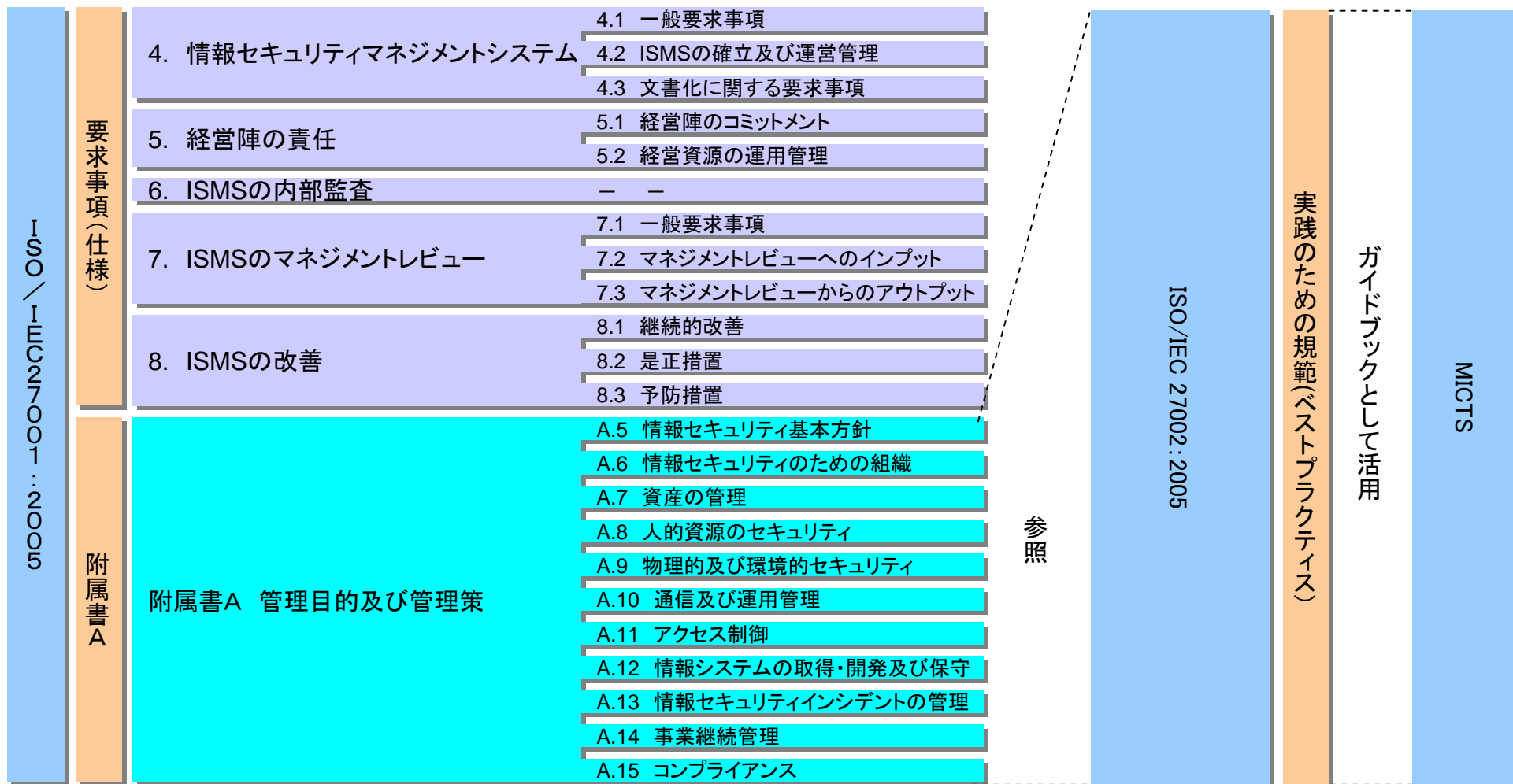




參考資料

1. 情報セキュリティ分野に関する既存の基準・ガイドラインの構造

ISO/IEC27001は、情報セキュリティマネジメントシステム構築に際して組織が遵守すべき要求事項(仕様)と附属書A(管理策)からなり、ISO/IEC27002は、附属書Aのベストプラクティスを集めたガイドラインとして位置付けられる。MICTSは、ISO/IEC27000シリーズのガイドブックとして位置付けられており、将来、ISO27000シリーズへ組み込まれる予定。(一部組み込み済み)

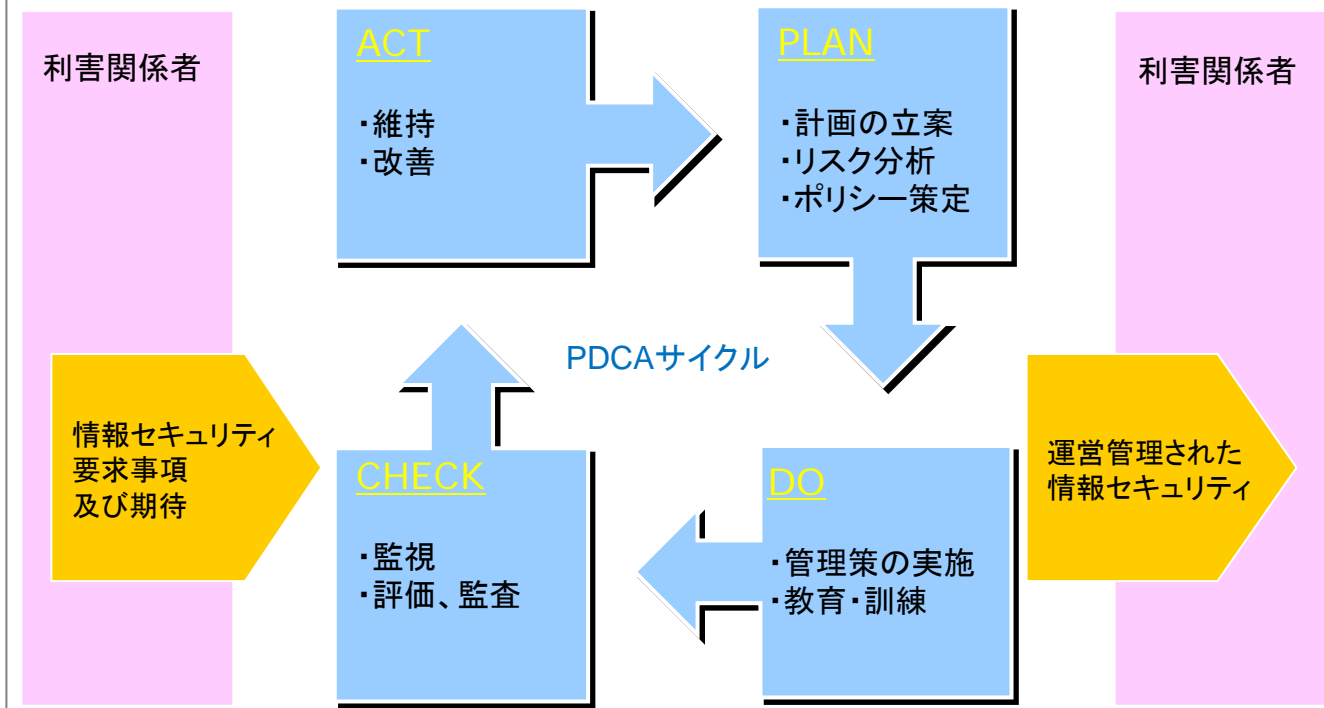


ISO/IEC 27001:2005の概要

ISO/IEC 27001は情報セキュリティマネジメントシステムの要求事項として、組織が所有する情報資産を機密性・完全性・可用性の観点から適切管理するための包括的な枠組みを提供している。コンピュータシステムのセキュリティ対策だけでなく、情報を扱う際の基本的な方針(情報セキュリティポリシー)や、それに基づいた具体的な計画、その実施と運用、一定期間毎の運用の評価や見直しまでを含めたトータルなセキュリティ管理体系の構築を要求している。

ISO/IEC 27001の原型はBS 7799であり、Part1(ガイド)とPart2(認証基準)で構成され、BS 7799のPart2はISO/IEC 27001、Part1はISO/IEC 27002として国際規格化されている。ISMS適合性評価制度においては、第三者である審査登録機関が本制度の認証を希望する事業者の適合性を評価する基準として使用されている。

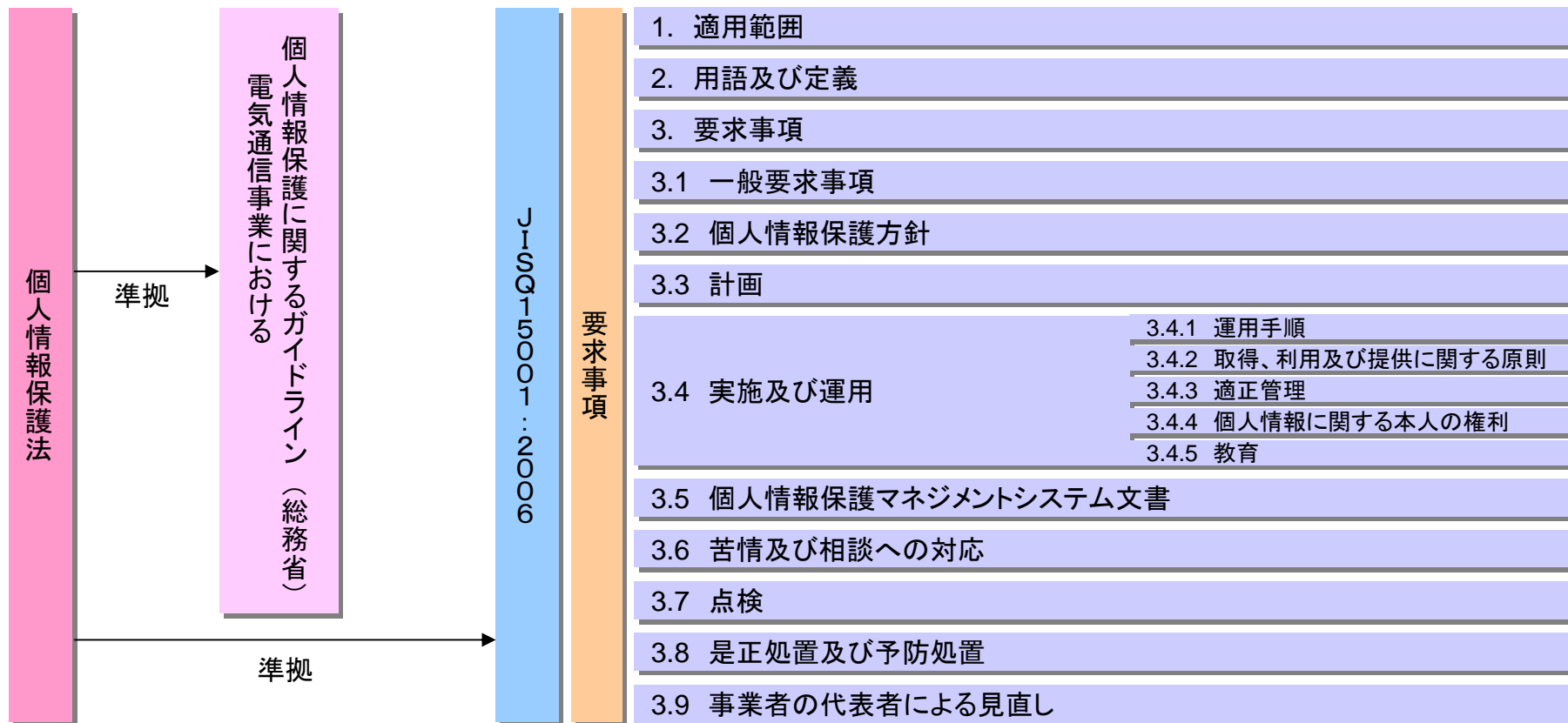
○ PDCAモデルによるプロセスアプローチ



ISO/IEC 27001:2005	要求事項(仕様)	4. 情報セキュリティマネジメントシステム
		5. 経営陣の責任
		6. ISMSの内部監査
		7. ISMSのマネジメントレビュー
	附属書A	8. ISMSの改善
		A.5 情報セキュリティ基本方針
		A.6 情報セキュリティのための組織
		A.7 資産の管理
		A.8 人的資源のセキュリティ
		A.9 物理的及び環境的セキュリティ
		A.10 通信及び運用管理
		A.11 アクセス制御
		A.12 情報システムの取得・開発及び保守
		A.13 情報セキュリティインシデントの管理
		A.14 事業継続管理
A.15 コンプライアンス		

2. 個人情報保護に関する既存の基準・ガイドラインの構造

個人情報保護分野に関する既存の基準・ガイドラインの構成・章立て及び関係は、以下のように整理される。



個人情報保護法の概要

個人情報保護法(平成15年法律第57号)は、全56条に附則が付けられており、第1章から第3章までが個人情報保護の基本法部分を構成し、第4章以下は民間部門を対象として具体的な権利義務を規定した一般法部分となっている。

第一章 総則

- 第一条(目的)
- 第二条(定義)
- 第三条(基本理念)

第二章 国及び地方公共団体の責務等

第三章 個人情報の保護に関する施策等

第一節 個人情報の保護に関する基本方針

第二節 国の施策

第三節 地方公共団体の施策

第四節 国及び地方公共団体の協力

第四章 個人情報取扱事業者の義務等

第一節 個人情報取扱事業者の義務

- 第十五条(利用目的の特定)
- 第十六条(利用目的による制限)
- 第十七条(適正な取得)
- 第十八条(取得に際しての利用目的の通知等)
- 第十九条(データ内容の正確性の確保)
- 第二十条(安全管理措置)
- 第二十一条(従業者の監督)
- 第二十二条(委託先の監督)
- 第二十三条(第三者提供の制限)

- 第二十四条(保有個人データに関する事項の公表等)
- 第二十五条(開示)
- 第二十六条(訂正等)
- 第二十七条(利用停止等)
- 第二十八条(理由の説明)
- 第二十九条(開示等の求めに応じる手続)
- 第三十条(手数料)
- 第三十一条(個人情報取扱事業者による苦情の処理)
- 第三十二条(報告の徴収)
- 第三十三条(助言)
- 第三十四条(勧告及び命令)
- 第三十五条(主務大臣の権限の行使の制限)
- 第三十六条(主務大臣)第三十六条

第二節 民間団体による個人情報の保護の推進

第五章 雑則

第六章 罰則

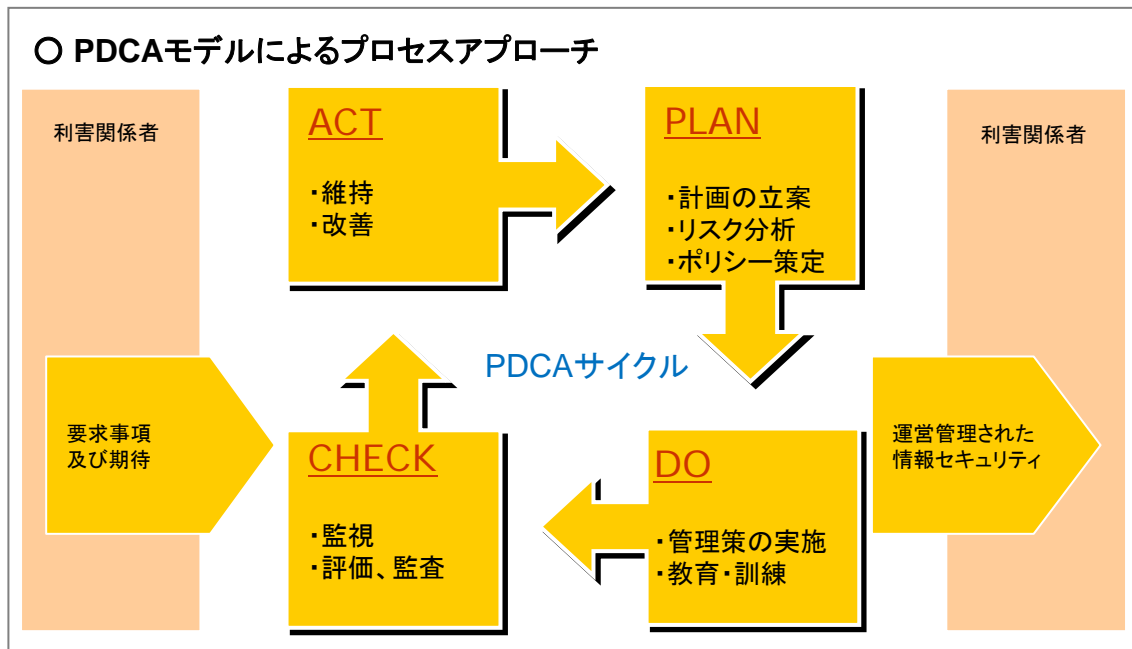
- 第五十六条
- 第五十七条
- 第五十八条
- 第五十九条

附 則 抄

JIS Q15001:2006の概要

JIS Q 15001は個人情報保護マネジメントシステムの要求事項として、事業者が所有する個人情報を持定し、その入手から廃棄に至る一連の個人情報の取扱いを適切管理するための包括的な枠組みを提供している。コンピュータシステムに保存されている個人情報のみならず、記録媒体や紙媒体等を含めた個人情報を扱う際の基本的な方針（個人情報保護方針）や、それに基づいた具体的な計画、その実施と運用、一定期間毎の運用の評価や見直しまでを含めたトータルな個人情報保護管理体系の構築を要求している。

JIS Q 15001はOECDプライバシーガイドラインの影響を大きく受けており、個人情報保護法施行後に規格の改定が行われJIS Q 15001:2006として同法律との親和性が一層高まった内容になっている。プライバシーマーク制度においては、第三者である審査登録機関が本制度の認証を希望する事業者の適合性を評価する基準として使用されている。



JIS Q15001:2006の個人情報保護法への対応

JIS Q15001は、もともとOECDのプライバシーガイドラインの影響を受けて策定されたものである。その後、新規格JIS Q15001:2006として個人情報保護法との親和性が一層高まっている。本規格を遵守することで、個人情報保護法も遵守することができるようになっている。基本的な枠組みは、ISO/IEC27001と同様にPDCAサイクルの運用になるが、3、4.3.1、4.4、4.6章には、個人情報保護分野特有の基準が設けられている。

1	適用範囲
2	引用規格
3	用語及び定義
4	要求事項
4.1	一般要求事項
4.2	個人情報保護方針
4.3	計画
4.3.1	個人情報の特定
4.3.2	法令、国が定める指針及びその他の規範
4.3.3	リスクなどの認識・分析及び対策
4.3.4	資源、役割、責任及び権限
4.3.5	内部規程
4.3.6	計画書
4.3.7	緊急事態への準備
4.4	実施及び運用
4.4.1	運用管理
4.4.2	取得・利用及び提供に関する原則
4.4.2.1	利用目的の特定
4.4.2.2	適正な取得
4.4.2.3	特定の機微な個人情報の取得の制限
4.4.2.4	本人から直接書面によって取得する場合の措置
4.4.2.5	個人情報を4.4.2.4以外の方法によって取得した場合の措置
4.4.2.6	利用に関する措置
4.4.2.7	本人にアクセスする場合の措置
4.4.2.8	提供に関する措置

4.4.3	適正管理
4.4.3.1	正確性の確保
4.4.3.2	安全管理措置
4.4.3.3	従業員の監督
4.4.3.4	委託先の監督
4.4.4	個人情報に関する本人の権利
4.4.4.1	個人情報に関する権利
4.4.4.2	開示などの求めに応じる手続き
4.4.4.3	開示対象個人情報に関する周知など
4.4.4.4	開示対象個人情報の利用目的の通知
4.4.4.5	開示対象個人情報の開示
4.4.4.6	開示対象個人情報の訂正、追加又は削除
4.4.4.7	開示対象個人情報の利用又は、提供の拒否権
4.4.5	教育
4.5	個人情報保護マネジメントシステム文書
4.5.1	文書の範囲
4.5.2	文書管理
4.5.3	記録の管理
4.6	苦情及び相談
4.7	点検
4.7.1	運用の確認
4.7.2	内部監査
4.8	是正措置及び予防措置
4.9	事業者の代表者による見直し

3. 内部統制に関する既存の基準・ガイドラインの概要

内部統制に関する既存の基準・ガイドラインは、以下のように抽出・整理できる。

COBIT (IT Governance Institute)

企業・自治体といった組織のITガバナンスの指針として、米国の情報システムコントロール協会 (ISACA) などが提唱するITガバナンスの実践規範のこと。フレームワークやガイドライン、成熟度モデル、ツールセットなどの一連の資料からなる。IT投資の評価、ITのリスクとコントロールの判断、システム監査の基準などに使われる。

SAS70 (米国公認会計士協会)

米国監査基準第70号。米国公認会計士協会 (AICPA) が定めた、アウトソーシングサービスなどの受託業務に関する内部統制を評価するための監査基準。受託業務を実施している企業は、SAS70に基づいて作成された報告書を提示すれば、組織の内部統制の仕組みが有効であることを委託者に認知されることが可能となる。

Web Trust (米国公認会計士協会)

WebTrustは、ECサイトのようなインターネットを利用した電子商取引を実施する事業者の内部統制について、実務慣行を基礎として定められたWebTrust原則および基準に準拠しているかを公認会計士が検証するサービス。主としてインターネットビジネスにおける利用者保護のための保証業務となっている。

Sys Trust (米国公認会計士協会)

SysTrustは、電子商取引に限定されず、企業の情報システムの内部統制についてSysTrust原則および基準にもとづき特定の期間において有効に運用されているかを公認会計士が検証するサービス。

4. SLAに関する既存の基準・ガイドラインの概要

SLAに関する既存の基準・ガイドラインは以下のように整理できる。

公共ITにおけるアウトソーシングに関するガイドライン (総務省)

電子自治体の構築にあたり、自治体間のシステム共同化、業務を民間へアウトソーシングする際必要となるプロジェクト、契約関係、SLAの内容について定めたガイドライン(2003年3月策定)

情報システムに係る政府調達へのSLA導入ガイドライン (経済産業省)

「情報システムに係る政府調達府省連絡会議」において決定された事項のうち、「調達管理の適正化」に関する具体例を示すため、SLAの重要性とその作成、発展のステップが盛り込まれたガイドライン。本ガイドラインは、「ITサービスの質を定量的に評価する尺度の確立」を目的としている。

電子自治体 基幹系SLA設定例 (2006年 ASPIC Japan編 ASP・IDC活用による 電子自治体アウトソーシング 実践の手引き)

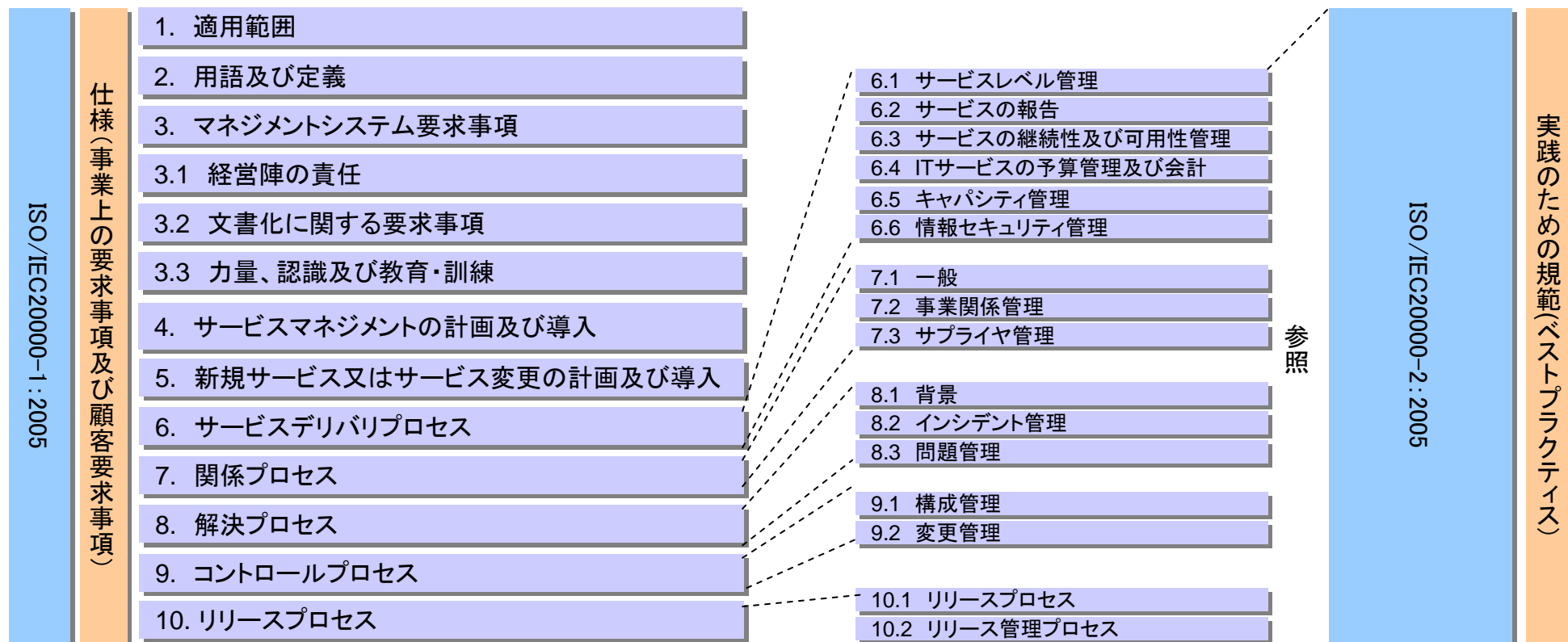
総務省にて策定された「公共ITにおけるアウトソーシングに関するガイドライン」の流れを受け、電子自治体構築におけるASP・IDCの有効活用を促進するために、それらの課題や進め方を解説した「ASP・IDC活用による電子自治体アウトソーシング 実践の手引」の基幹系SLA設定例として作成されたガイドライン

民間向けITシステムのSLAガイドライン 第3版 (2006年 日本情報技術産業協会 JEITA)

既にガイドラインとして確立されていた、さまざまなガイドラインの流れを受け、JEITAは、SLA/SLM専門委員会を設置し、民間向けSLAの標準化活動を開始。その活動成果として、民間におけるSLAの共通指標を提示、ITサービスの利用者と供給者の間で適切なレベル選択が可能となることをめざしたガイドライン

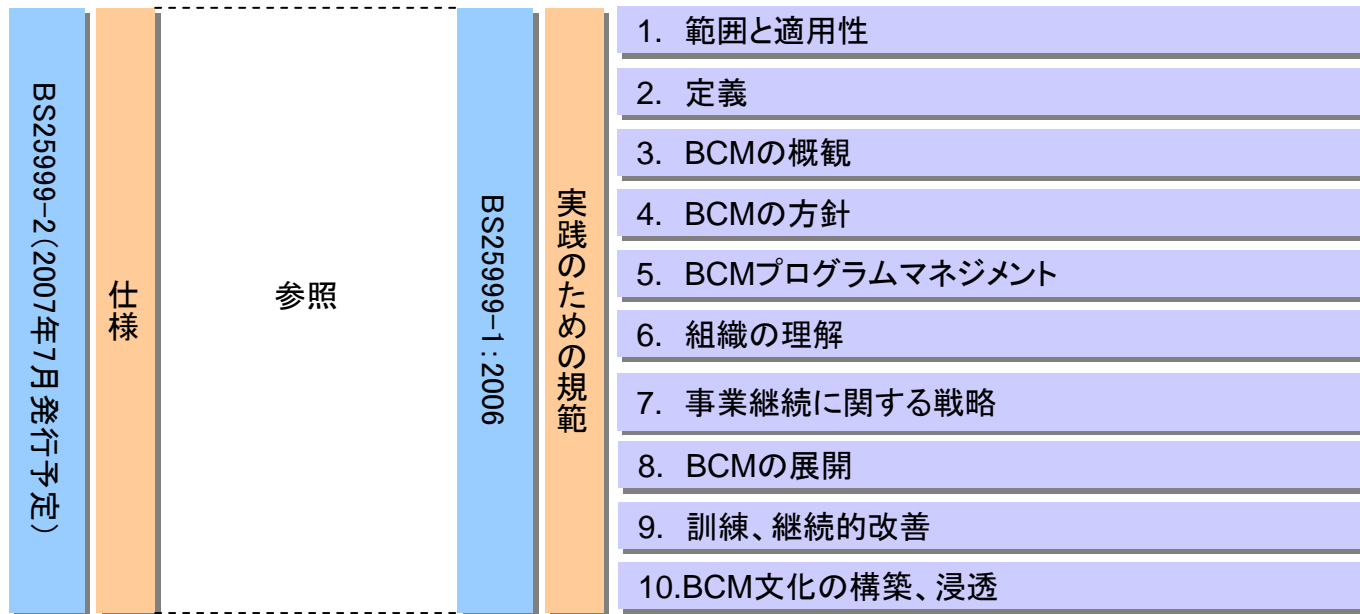
5. ITサービスに関する既存の基準・ガイドラインの構造

ITサービス分野に関する既存の基準・ガイドラインの構成・章立て及び関係は、以下のように整理できる。



6. 事業継続に関する既存の基準・ガイドラインの構造

事業継続分野の基準・ガイドラインで、今後ISO化の可能性が高いBS25999-1の構成・章立て及びBS25999-2との関係は、以下のように整理できる。



事業継続・信頼性に関する既存の基準・ガイドラインの概要

事業継続・信頼性分野に関する既存の基準・ガイドラインの概要を以下に示す。

事業継続ガイドライン 第一版（内閣府防災担当）

企業に対して事業継続の取組みの概要および効果を示し、防災のための社会的な意義や取引における重要性の増大、自社の受けるメリット等を踏まえて企業が自主的に判断するのを促すことを目的として策定されたガイドライン。ガイドラインには、具体的な取組みを簡易にチェックできるように、「事業継続ガイドライン チェックリスト」が用意されている。(2005年8月策定)

事業継続計画策定ガイドライン（経済産業省）

IT事故を想定した事業継続計画の策定手順や検討項目をわかりやすく解説することを念頭に策定されたガイドライン。内容は、①事業継続策定に際しての基本的な考え方、②策定時に考慮すべき総論的事項、③事業継続計画策定に当たっての具体的検討事項、④IT事故を想定したケーススタディ及び⑤参考資料としてベストプラクティス事例等が盛り込まれている。(2005年8月策定)

中小企業BCP策定運用指針（中小企業庁）

自然災害や大火災等の緊急事態において事業中断を最短にとどめ被害を最小化するための企業の危機管理の新技术として、主に欧米で発達し普及しているBCPの策定と運用のノウハウを我が国の中小企業向けに初めてわかりやすく解説した指針

金融機関等におけるコンティンジェンシープラン 策定のための手引書(金融情報システムセンター)

大規模な自然災害や不慮の事故等といった不測の事態が発生した場合にも、業務の継続を図る手段を講じるため、あらかじめ各金融機関等がコンティンジェンシープラン(災害時の緊急時対応計画)を作成する際の手引書

情報通信ネットワーク安全・信頼性基準 (昭和62年郵政省告示第73号)

情報通信の健全な発展とその安全・信頼性の向上を図ることを目的として定められたガイドライン。登録の対象となる情報通信ネットワークは、第二種電気通信事業の用に供する情報通信ネットワークや電子計算機を用いて計算、検索その他情報処理を行うオンライン情報処理業のネットワークなど。