社員一人一人が　　セキュリティ
～企業情報管理(ｾｷｭﾘﾃｨ)法～

２００８．５．１２

弁護士法人　エルティ総合法律事務所
所長弁護士／システム監査技術者／
公認システム監査人
藤　谷　護　人

1.「仕事」としての「情報セキュリティ対策」

(1)「仕事」とは？

□□を○○することである。

(2)「問題」とは？

ＡＡＡＡＡとＢＢとのＣＣＣＣである。

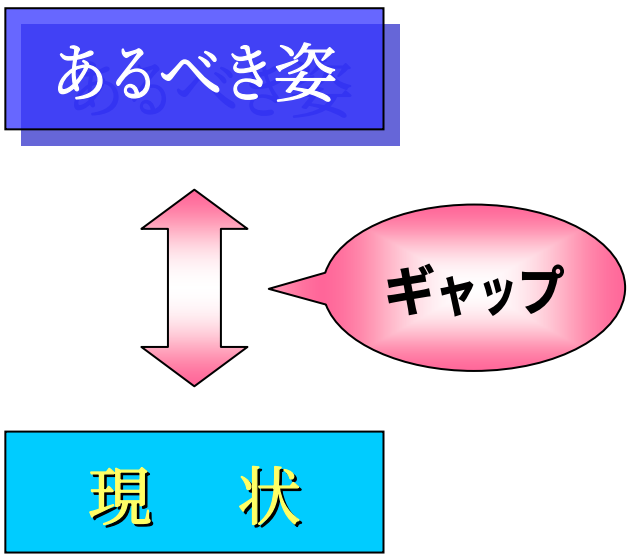
(3)「解決」とは？

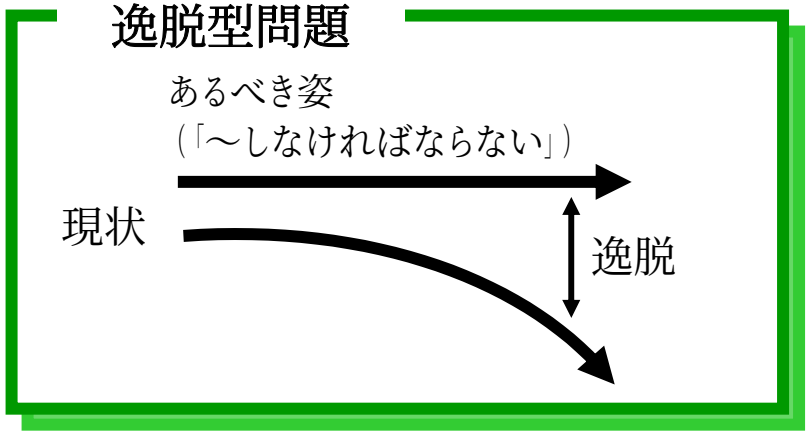
□□をＤＤし、ＥＥし、ＦＦし、ＧＧすることである。

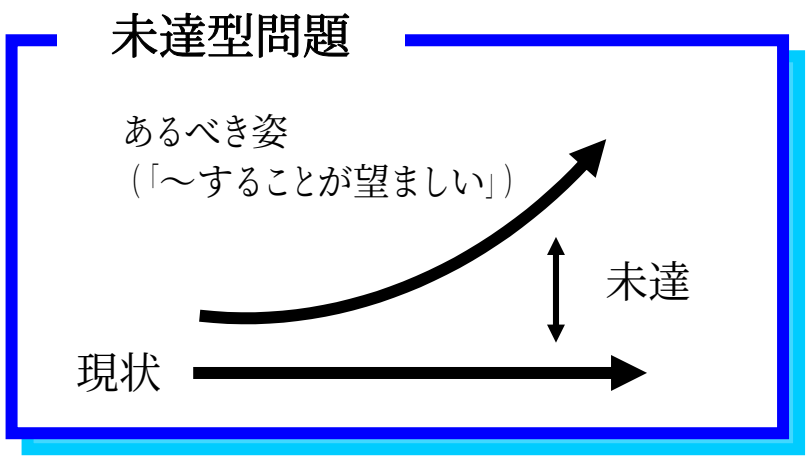
(4)「情報セキュリティ対策」とは？

逸脱型問題と未達型問題

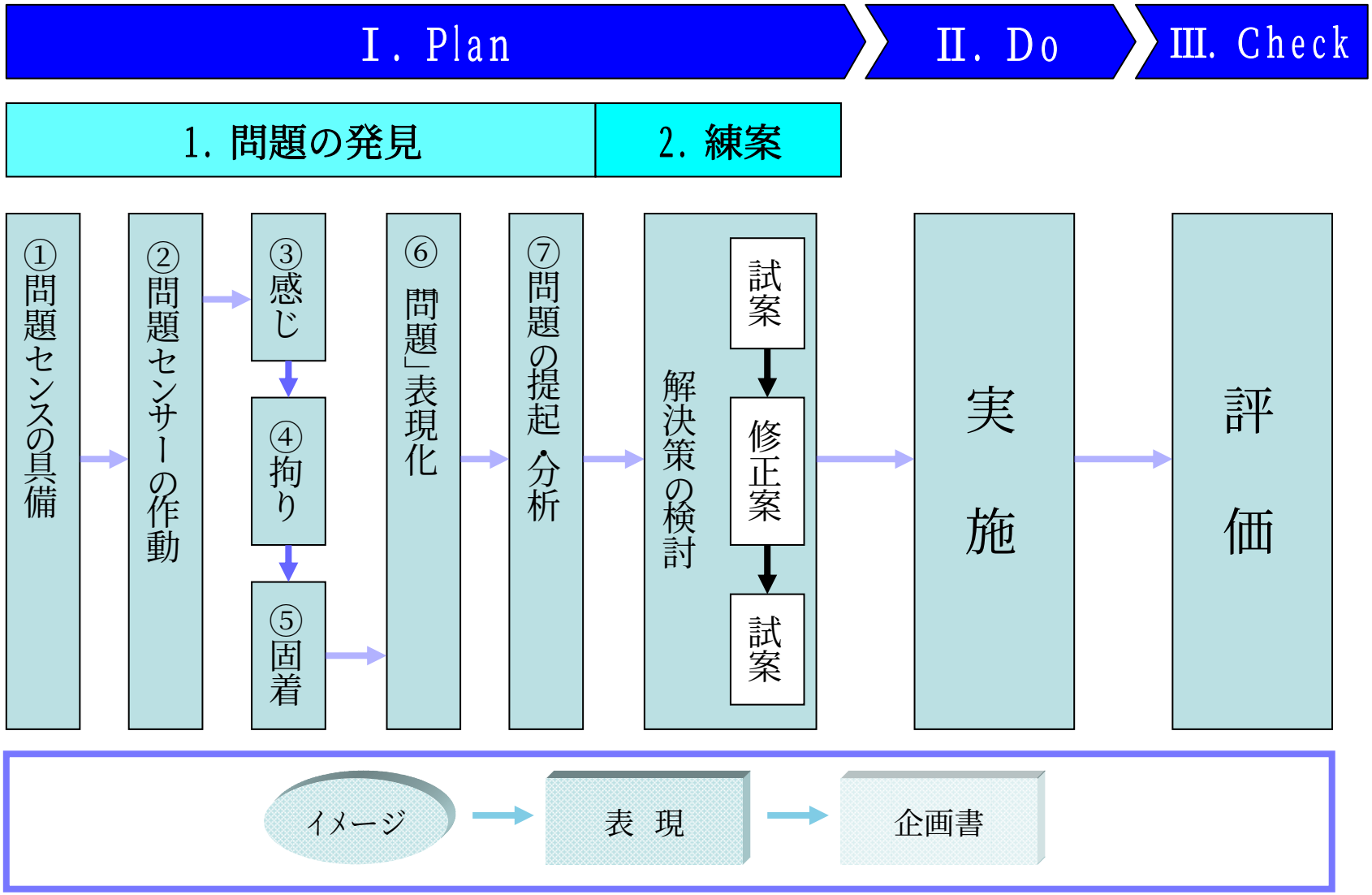
問題とは・・・・・・







問題解決のプロセス



2．情報セキュリティ・問題解決技法としての「情報セキュリティ・リスクマネジメント」とは？

(1)「情報セキュリティ」とは？

「情報資産」について、CIA+ＡＣを図ること

①機密性Confidenciality　②完全性Integrity　③可用性Availability

④説明責任性Accountability　⑤法令遵守性Compliancy

(2)情報セキュリティ・「リスク」とは？

「管理策」の「脆弱性」を「脅威」が突破して、

「情報資産」の「価値（CIA）」が損なわれる危険性

(3)「リスクマネジメント」とは？

「リスク分析」

「リスクコントロール」

・抑制／防止→検出→回復

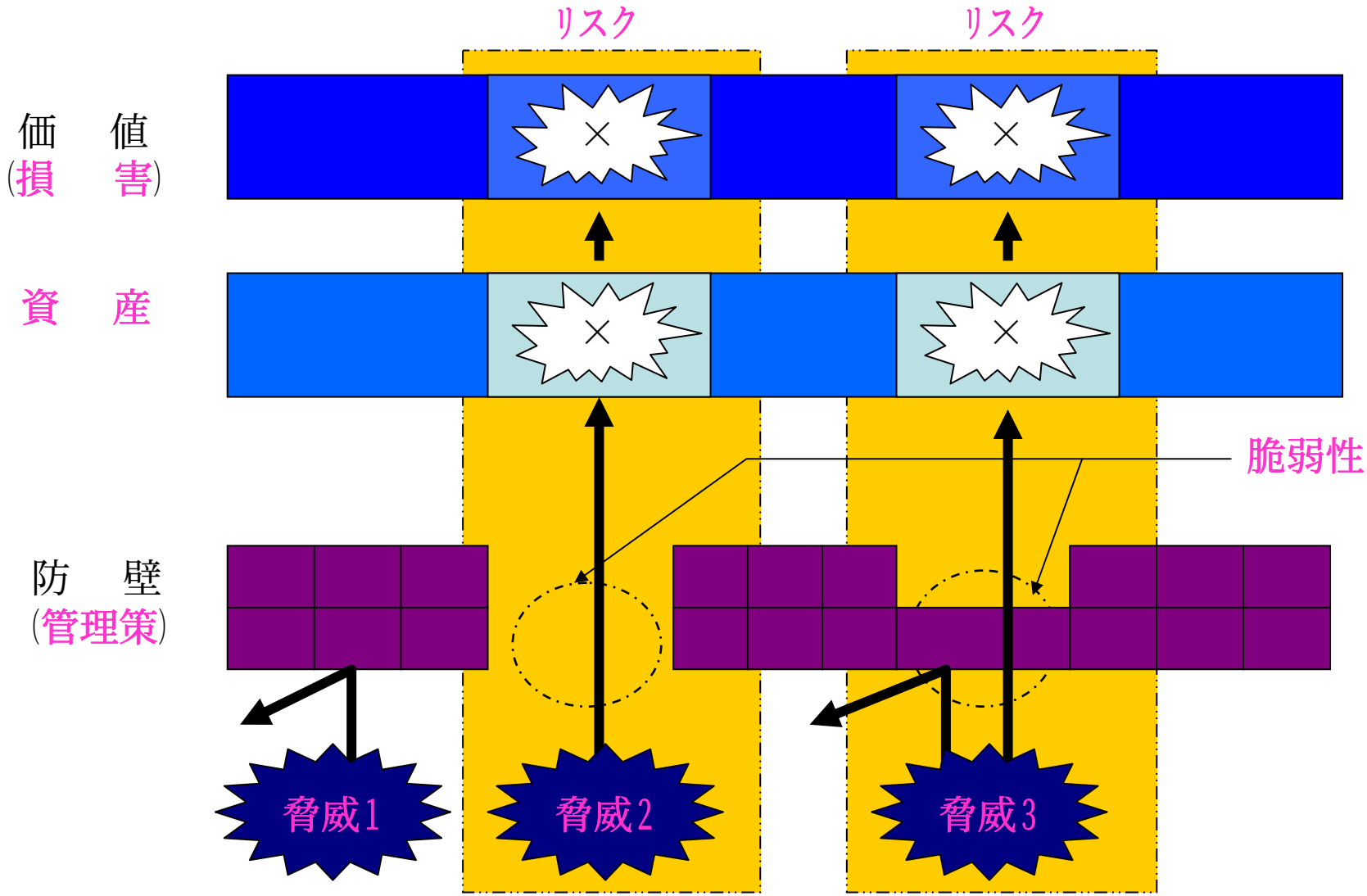
・低減／移転／回避／保有（監視）

「数値化」

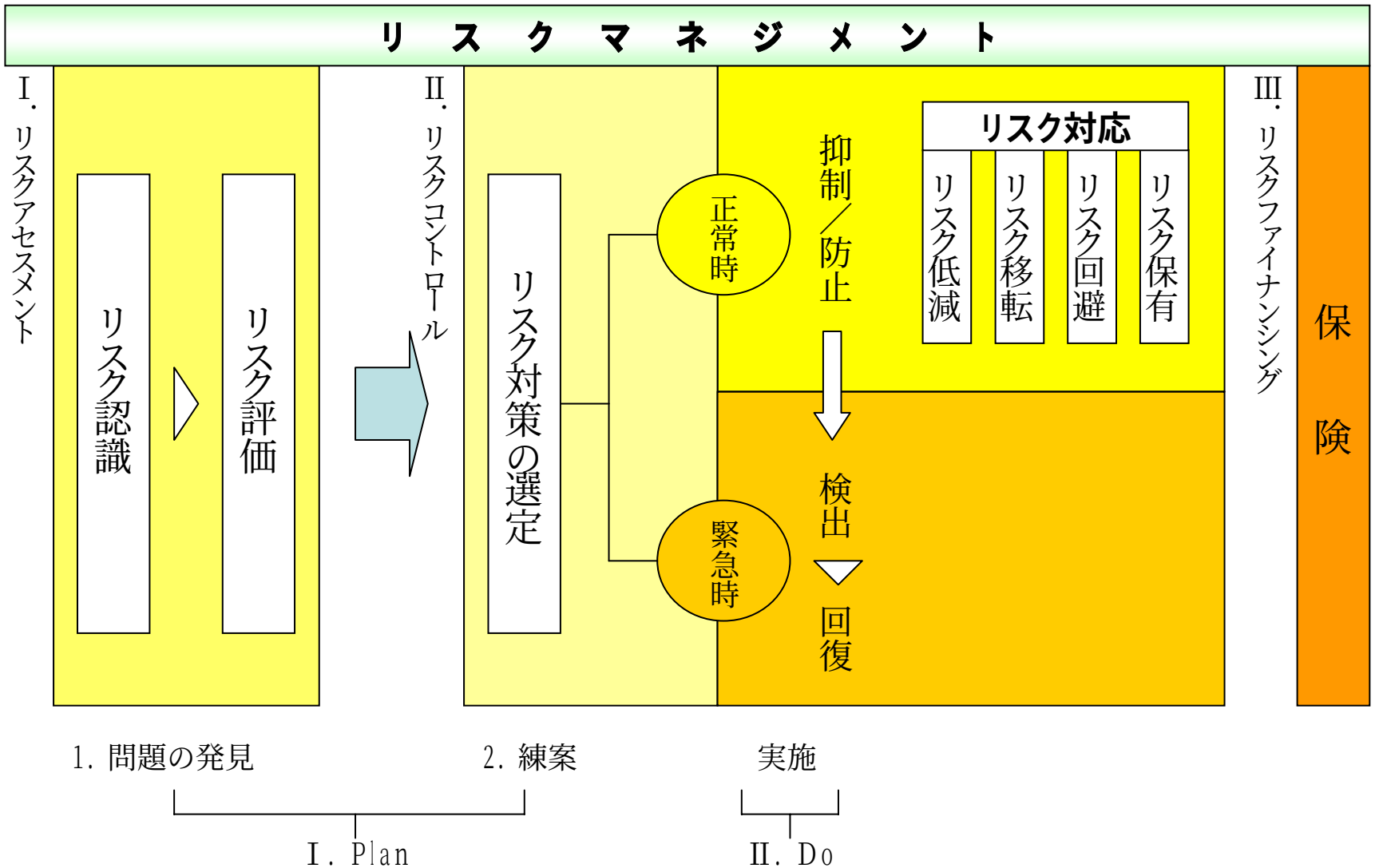
(4) 内部統制原理

(5) ＩＳＭＳ

＜資産と管理策と脅威と脆弱性とリスクの相関関係＞

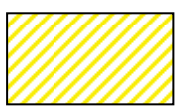


リスクマネジメント技法



リスク値算出早見表

	脅威								
	1			2			3		
	脆弱性								
資産価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2		4	6	4	8	12	6	12	18
3		6	9	6	12	18	9	18	27
4		8	12	8	16	24	12	24	36

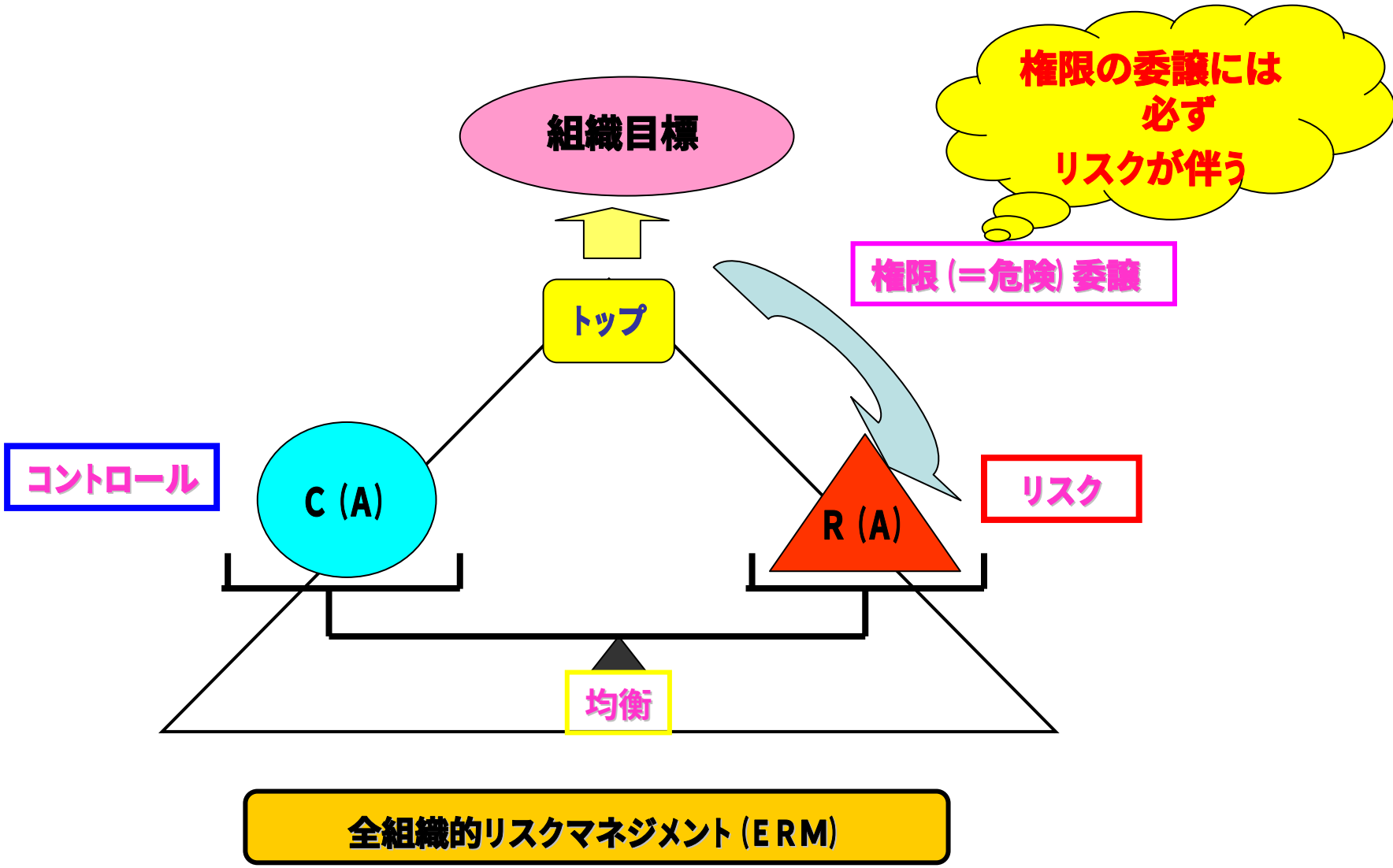


許容リスク値は「8」以下の例。資産価値4、リスク値「24」を許容リスク値「8」にするには、2つの方法がある。

「情報セキュリティ」は「何故」必要なのか

- 情報システムは「技術」である。デメリットを伴わない技術はない。
- 「社会的に許す法理」＝技術の「有用性」を社会的に必要としており、技術のデメリットによる「リスクをコントロール」できる場合には、その技術の使用を認める、という考え方。
- 「自動車技術」には、毎年交通事故死者が1万人というリスクがある。だから自動車技術を使用することは「原則として禁止」されている。「運転免許」とは、交通法規の理解と安全運転技術の修得を条件として「禁止を解除」すること。
- 「コンピュータやインターネット技術」にも情報漏えいやネット自殺などデメリットがあるが。その使用は「原則として自由」である。しかしそれを安全有効に使用するためには「情報セキュリティ（機密性（C）・完全性（I）・可用性（A）・説明責任性（A））」が不可欠である。
- ＪＳＯＸ法により「内部統制システム整備義務」として「情報セキュリティ」が法的義務化（統制の対象たるリスクの主要なものとして「情報セキュリティリスク」が位置づけられる故）された。

「内部統制原理図」



全組織的リスクマネジメント（ERM）

「内部統制原理」とは

■組織とは、組織目標の実現のために、人的資源と物的資源を有機的に結合して、諸活動を行う社会的存在である。

■人的資源の有機的結合は、トップから下位への権限委譲によって行われる。

■この権限委譲によって、個人活動を遙かに超えた組織的活動が可能になり、大きな成果を実現することが可能になる。

■しかし「権限委譲には必ずリスクの委譲が伴うものである」（権限の付与はリスクの付与でもある）ことに気付かなければならない。

■リスクの大きさと均衡のとれた管理策（コントロール）を実施（リスクマネジメント）しなければ、リスクが顕在化してしまう。

■組織が社会的存在として許されるためには、社会（あるいは組織に対する様々なスタークホルダー）に対して、迷惑を掛けかねない組織のリスクをマネジメントする仕組み（エンタープライズ・リスクマネジメント＝内部統制のシステム）を整備することが要件である（社会的に許す法理）。

■以上の社会的原理を、組織の「内部統制原理」と言い、内部統制原理に基づいて組織管理を実現するシステムとはＥＲＭシステムそのものに他ならないのである。

J-Sox法のルーツ①（商法・会社法的リスク）

○経営者の「内部統制（不作為）責任」を問う株主代表訴訟
＝「取締役の善管注意義務違反」判例ルール

①H12.9.20 大和銀行株主代表訴訟事件、大阪地裁判決
「健全な会社経営を行うためには、～リスク管理が欠かせず、会社が営む事業の規模、特性に応じたリスク管理体制（いわゆる内部統制システム）を整備することを要する」として、現・元取締役らに総額８３０億円の賠償命令。

②H15.4.5 神戸製鋼所株主代表訴訟事件、神戸地裁和解所見「取締役は違法行為などがなされないよう、内部統制システムを構築すべき法律上の義務がある。企業トップは、社内の違法行為について知らなかったという弁明だけでその責任を免れない」として元会長らが3億1０００万円払うとの和解成立。

H15.6.27　経済産業省、リスク管理・内部統制に関する研究会報告書「リスク新時代の内部統制　－リスクマネジメントと一体となって機能する内部統制の指針－」公表。

H15．7．30　旧商法特例法において、委員会設置会社における取締役会に「内部統制システム整備義務」を規定。＜資料3＞

H17.6.29 会社法の中に、委員会設置会社と大会社の取締役会に「内部統制システム整備義務」を規定＜資料1・2＞。それら以外の会社には判例ルール。

8．J-Sox法のルーツ②

米国	エンロン	ワールドコム
	2001.10 新聞報道（不正会計）	2002.6　2002.7 粉飾露見　破綻 監査法人コンサル部門が結託

日本	カネボウ	西武鉄道	ライブドア
	2005.4 粉飾露見	2004.10 有価証券報告書虚偽記載	2006.1 偽計取引 風説流布

Sox法
§303
§404

2005.12.8
「財務報告に係る内部統制の評価及び監査の基準のあり方について」
企業会計審議会

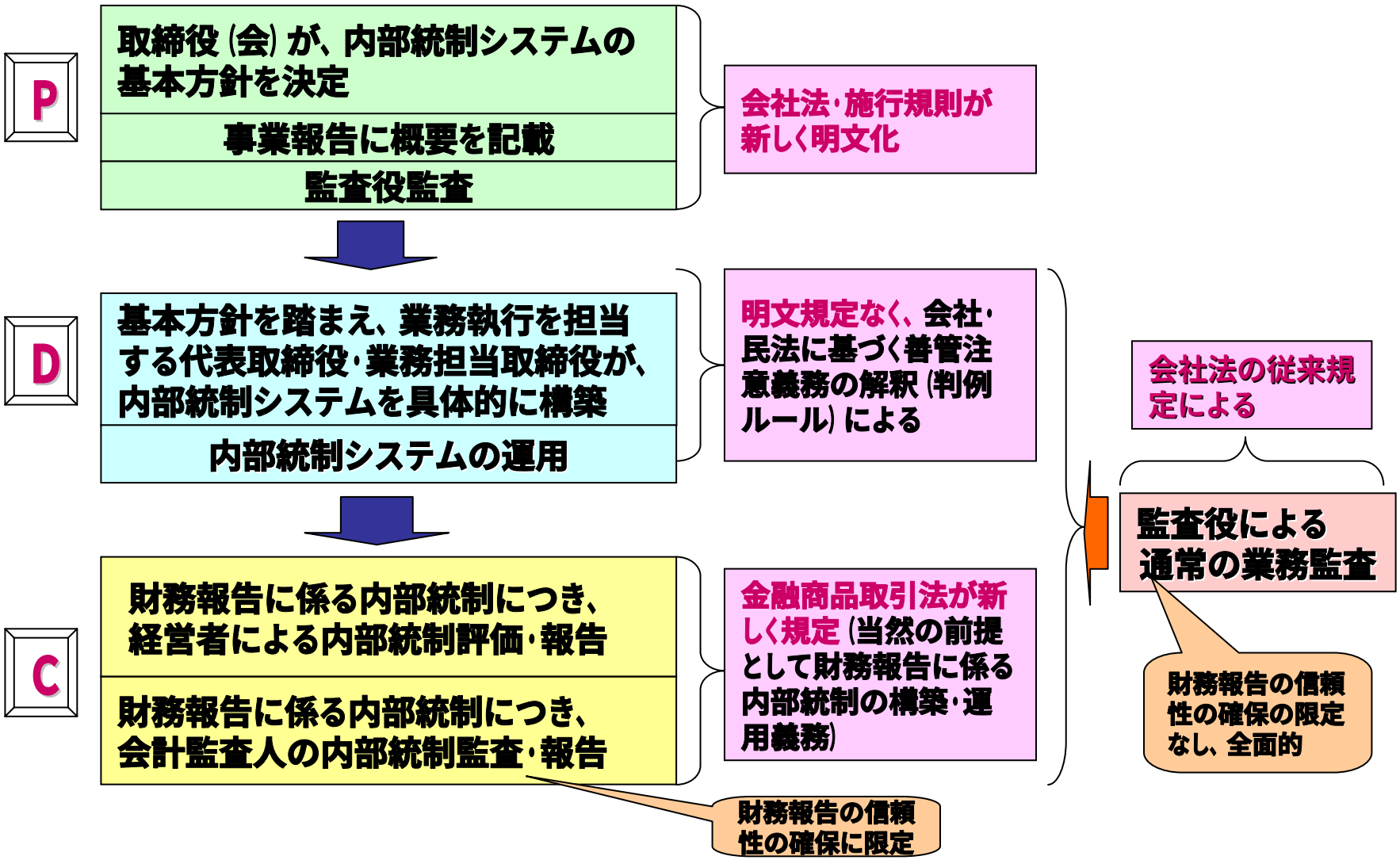
金融商品取引法
2006.6.7における
「第2章 企業内容等の開示」

2006.11.7
「実施基準（案）」
企業会計審議会

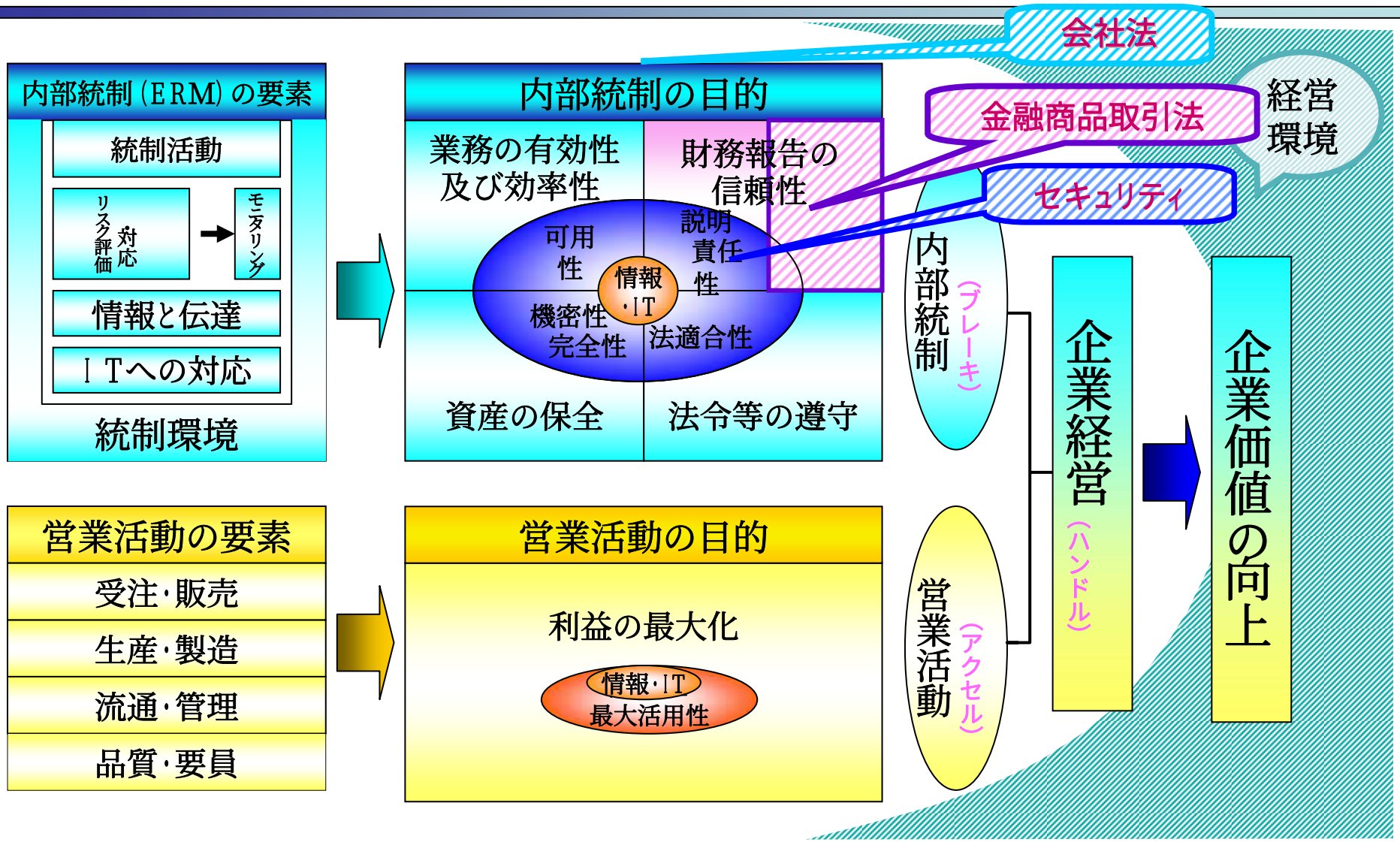
従来の
コーポレートガバナンス
が
機能不全

「内部統制システム」整備の義務化
→「業務プロセスの可視化」による
株式市場の信頼性の確保

「内部統制システム・マネジメントサイクル」と「対応法令・ルール」



会社活動の全体構造における「会社法」「金取法」の内部統制の位置付けと「情報・IT」「セキュリティ」との関係



「ITの統制目標」と「アサーション」の関係

IT の統制目標	アサーション（適切な財務情報を作成するための要件）
完全性 (Integrity)	網羅性、期間配分の適切性
正確性	実在性、評価の妥当性、期間配分の適切性、表示の妥当性
正当性	実在性、権利と義務の帰属、評価の妥当性

「アサーション」には存在しない「ITの統制目標」

- **機密性(Confidentiality)**
- **可用性(Availability)**

「アサーション」の上位に位置する「ITの統制目標」

- **説明責任性(Accountability)**
- **法適合性(Compliancy)**

金融商品取引法における「ITへの対応」に関する検討

◆「セキュア・ジャパン2006」（2006年6月15日　情報セキュリティ政策会議決定）

第2章　第4節

ウ）情報セキュリティ関連制度と内部統制制度等との整合性確保

（内閣官房、金融庁及び経済産業省）

「政府が推進する情報セキュリティに関する取組みについて、政府全体としての整合性を確保するため、現在構築が検討されている内部統制制度のIT統制に係る部分において、情報セキュリティ関連制度との関連を考慮しつつ、2006年度に検討を進める。」

■　金融商品取引法（金取法）の成立により、上場企業は、財務報告に係る内部統制の構築が求められることとなる。

■　「セキュア・ジャパン2006」に掲げられた上記の項目については、例えば、経済産業省が展開している既存の情報セキュリティ関連制度と内部統制制度のIT統制部分との間の整合性確保に係る検討があり得るのではないか。

	米国	日本
法律	SOX法	金融商品取引法
内部統制フレームワーク	PCAOB監査基準第2号（COSOフレームワーク）	財務報告に係る内部統制の評価及び監査の基準（企業会計審議会） 金融商品取引法
IT統制フレームワーク	COBT（その他ITIL、ISO/IEC17799等）＋IT Control Objectives for SOX	システム管理基準＋システム管理基準追補版

「情報化社会の進展」と「プライバシー問題」と「プライバシー権」

●19世紀末

マスメディアの発達 → マスメディア・プライバシー問題 → 「一人にしておかれる権利」

●1960年代～

コンピュータ化 → コンピュータ・プライバシー問題（＊国民総背番号制）

●1980年代～

ネットワーク化 → ネットワーク・プライバシー問題　　ＯＥＣＤ８原則

●現在

ネットワークの世界的発展 → 世界ネットワーク・プライバシー問題 → 「自己情報コントロール権」

1．個人情報保護法制整備の背景

我が国における官民通ずるIT社会の急速な進展

公的部門
- 電子政府・電子自治体の構築

民間部門
- 電子商取引の進展
- 顧客サービスの高度化　等

国際的な情報流通の拡大・IT化

OECD
　ほとんどの国で民間部門を対象にした法制を整備

情報の自由な流通とプライバシー保護の確保　→　制度間の調和の要請

IT社会の「影」

・プライバシー等の個人の権利利益侵害の危険性・不安感増大

官・民における個人情報保護法制の確立

→　保護と利用の調和

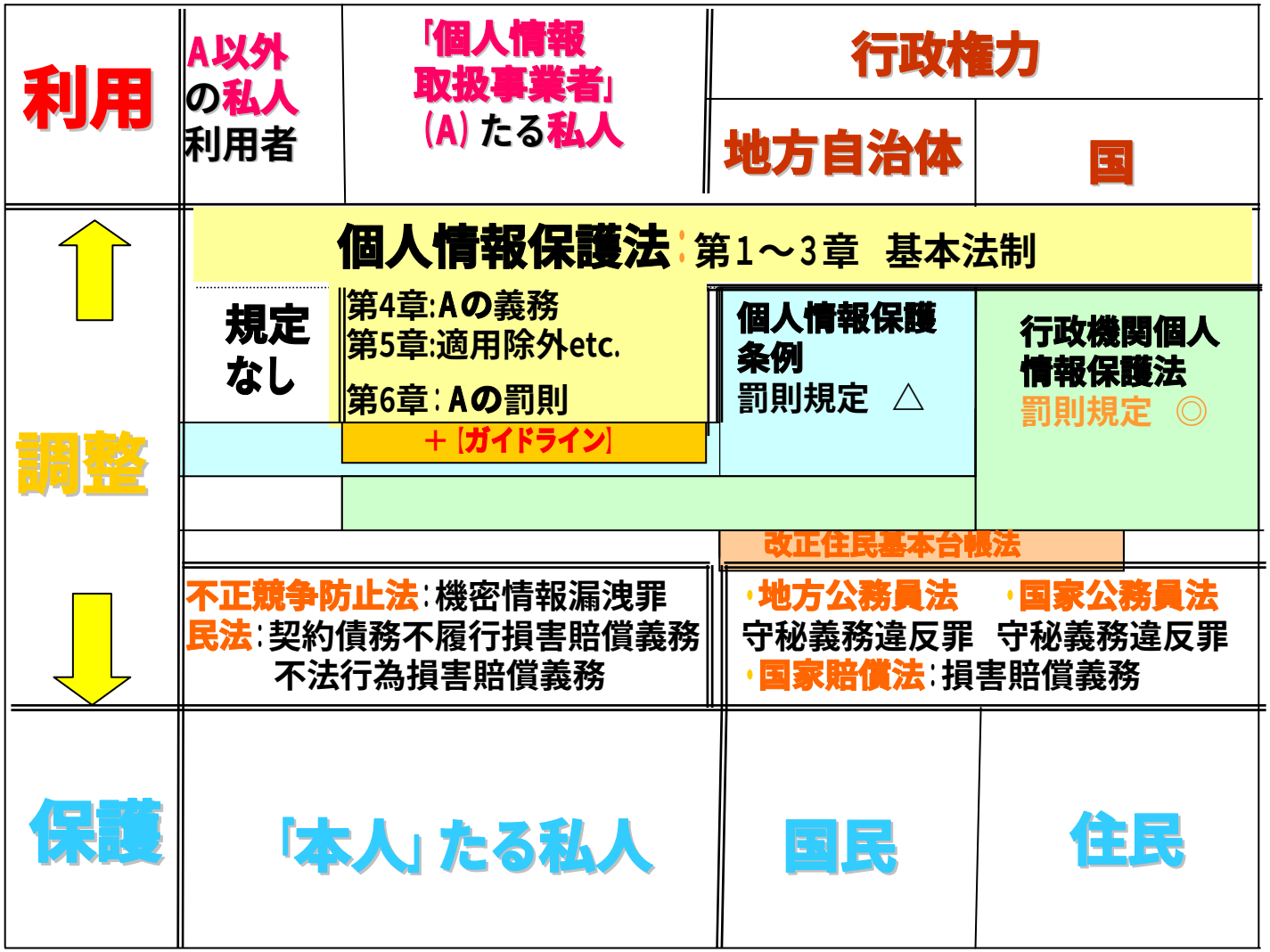
・基本理念

・国等の責務、施策
　→　基本法制（第1～3章）

・民間事業者が遵守すべき規律
　→　基本法制（第4章）

・公的機関（国・独立行政法人・地方公共団体等）が遵守すべき規律
　→　・行政機関法制
　　・独立行政法人法制
　　・条例

個人情報保護法制の概念図



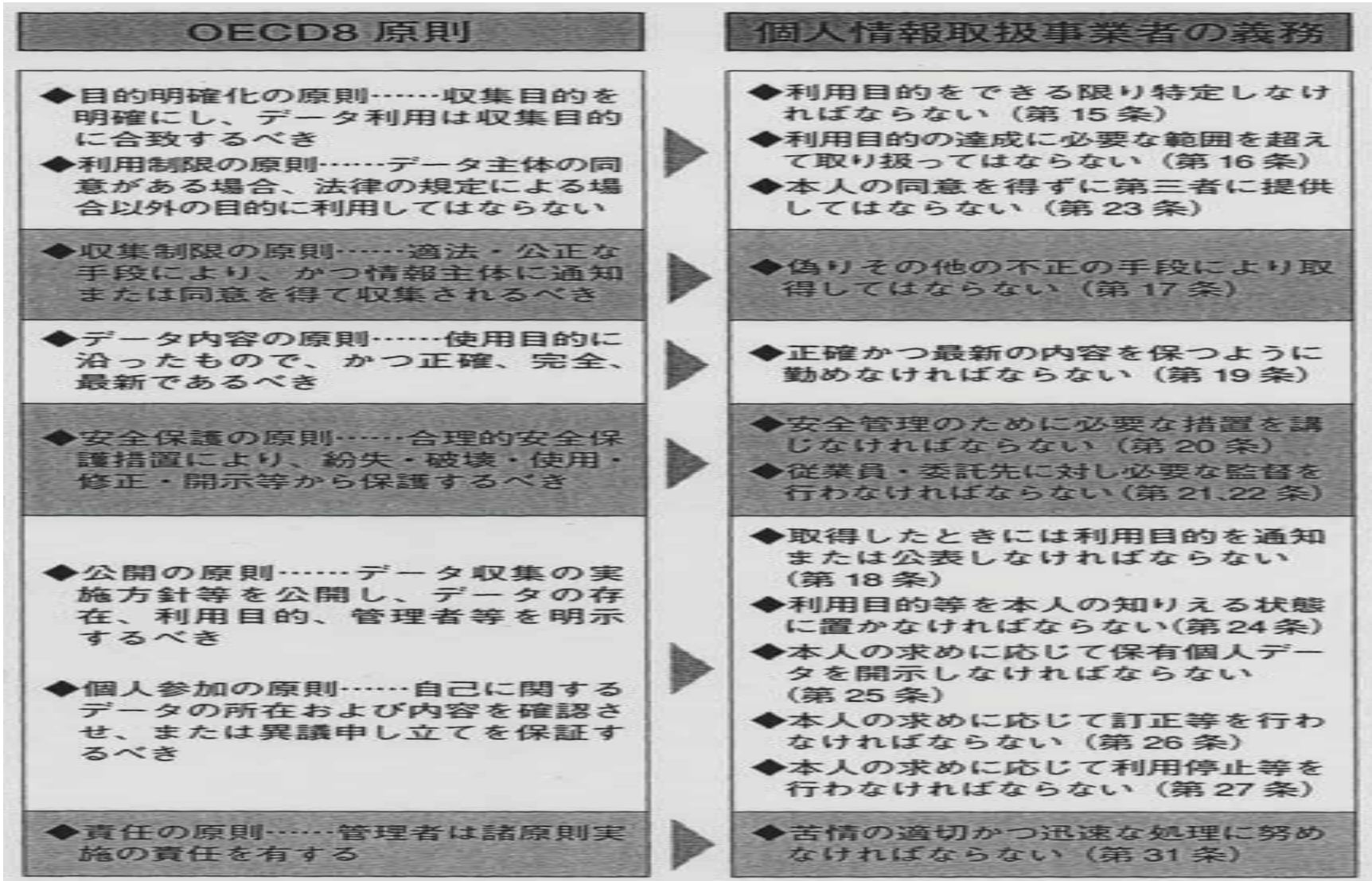
個人情報取扱事業者の義務規定における保護と利用との具体的調整
～反射的利益としての「自己情報コントロール機会」保障の程度～

		規定項目	個人情報の種類	自己情報コントロール権の行使機会の保障方法	個人情報取扱事業者にとっての負担の程度	注1
利用目的	15条	利用目的の特定	個人情報	Ⅰ. 合理的予想可能程度の特定	中	×
				Ⅱ. 目的変更の相当関連性	中	
	16条	目的外利用の禁止	個人情報	目的外利用には、あらかじめ同意が必要	重	○
	17条	不正取得の禁止	個人情報	－	重	○
	18条	取得時利用目的公示義務	個人情報	Ⅰ. 通知または目標	軽	○
				Ⅱ. 契約－利用目的明示	重	
				Ⅲ. 変更利用目的－通知または公表	軽	
セキュリティ	19条	正確性保持義務	個人データ	－	軽	×
	20条	安全管理措置義務	個人データ	－	中	○
	21条	従業者監督義務	個人データ	－	中	○
	22条	委託先監督義務	個人データ	－	中	○
第三者提供	23条	第三者提供の禁止	個人データ	Ⅰ. 第三者提供には、あらかじめ同意が必要	重	○
				Ⅱ. オプトアウトには、あらかじめ本人通知、または、本人が容易に知り得る状態	中	
				Ⅲ. 共同利用には、あらかじめ本人通知、または本人が容易に知り得る状態（4項3号）	中	
開示等	24条	利用目的公示義務	保有個人データ	Ⅰ. 本人が知り得る状態：（求めに応じて回答）	軽	○
				Ⅱ. 利用目的の通知	重	
	25条	開示義務	保有個人データ	Ⅰ. 開示	重	○
				Ⅱ. 不開示の通知	重	
	26条	訂正義務	保有個人データ	Ⅰ. 調査、訂正	重	○
				Ⅱ. 不訂正の通知	重	
	27条	利用停止義務	保有個人データ	Ⅰ. 16条違反、17条違反、利用停止	重	○
				Ⅱ. 23条違反、第三者提供停止	重	
				Ⅲ. 利用不停止の通知	重	
	28条	理由説明	保有個人データ		重	×
	29条	開示手続	保有個人データ		重	×
	30条Ⅰ	手数料	保有個人データ		－	×
苦情処理	30条Ⅱ	手数料の合理性	保有個人データ		中	○
	31条	苦情適切処理	－		重	×

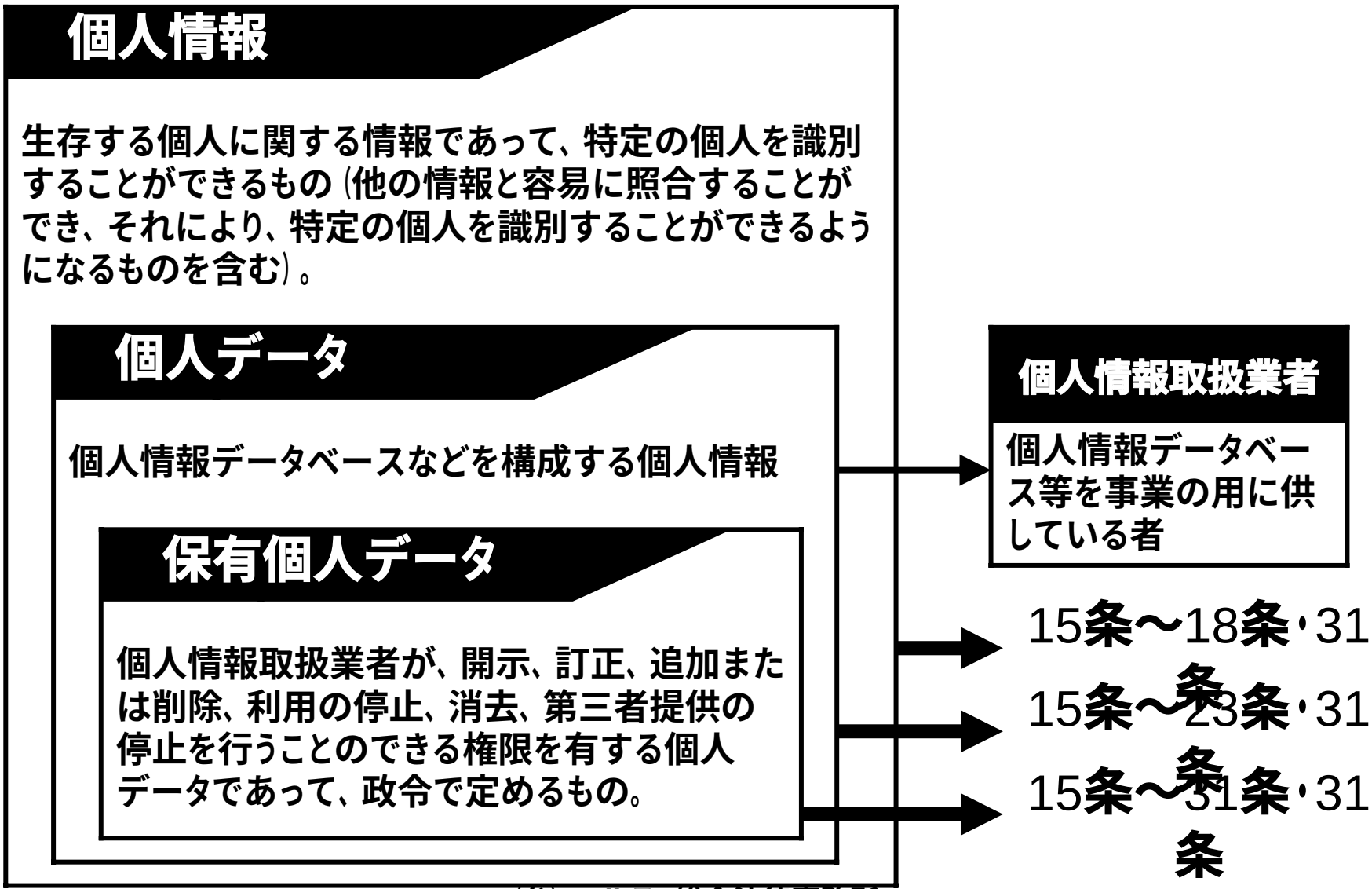
※自己情報コントロール権の行使機会の保障のために、事前に本人の同意を得る権利を「オプトイン方式」という。

注1：×印の条文の義務は、それに違反しても行政指導（勧告・命令）発動の対象とならない。従って、結果的には刑罰の対象とならない。その意味で訓示規定的な義務である。

OECD8原則との対応



「個人情報の種類」と個人情報取扱事業者



アウトソーシングと内部統制

1．アウトソーシングにおける個人情報漏洩事件の頻発

2．なぜか？①アウトソーシングによる内部統制力の喪失
②アウトソーシング先の内部統制力の不十分
③再委託

3．「アウトソーシングセキュリティ構造式」

$SL(X) \leqq SL(Y) \leqq SL(Z)$

$SL(X) = C(X) - R(X)$、$SL(Y) = C(Y) - R(Y)$、$SL(Z) = C(Z) - R(Z)$

$R(X) = R(Y) = R(Z)$、$C(X) \leqq C(Y) \leqq C(Z)$

SL=Security Level、C=Control、R=Risk

4．「アウトソーシング・セキュリティリスクマネジメント」

① $R(X) = R(Y) = R(Z)$

②アウトソーシング先が十分な「ISMS」を有していること

③喪失した統制力の補填：「関与制度」報告義務、監査権、改善要求権、完全損害賠償義務

④再委託にも①～③＋機関法53条は、事実上「再委託拒絶」

5．行政事務のアウトソーシングにおける「特別性」
→公務員の特別権力関係制の代替性確保：「指名」「みなし公務員」

6．共同アウトソーシングにおける「特別性」
→「共同」による統制主体力の低下克服：「共同組織（一部事務組合など）形成」

労働力形態による内部統制力喪失関係
→統制力におけるバルネラビリティ比較

		自社常用	自社契約	自社ﾊﾟｰﾄ	派　遣	委　託	再委託
帰属･服従意識		○	△	△	×	×	×
兼･競業禁止権		○	○	×	×	×	×
懲戒解雇権		○	○	○	×	×	×
懲戒権		○	○	○	×	×	×
研修命令権		○	○	○	×	×	×
規範遵守要求権		○	○	○	○	×	×
守秘要求権		○	○	○	○	○	△
誓約書徴求権		○	○	○	△	×	×
業務指揮命令権		○	○	○	○	×	×
監査権		○	○	○	×	×	×
改善指導命令権		○	○	○	×	×	×
損害賠償請求権	契約	○	○	○	×	○	×
	不法行為	○	○	○	○	○	○

主な情報漏洩事件　～組織の存亡に関わる重大問題～

- H6.12.7　東京都江戸川区で住民健康診断データ（含む病歴）9万人分が流出。
- H8.8.　全国信用情報センター連合会から83万人分流出。
- H10.1.29　テンプスタッフの登録9万人の個人データ（美人度ランキング含む）流出。
- H10.2.　高島屋から顧客情報50万人分流出。
- H11.5.22　宇治市全住民21万件の住民票データ流出。
- H13.8.16　小田急百貨店、社員が顧客情報38万人分持ち出し。
- H14.5.26　TBC　問い合わせ・相談をした顧客、アンケート回答者合計約51000人の相談内容などが流出。
- H14.8.6　富士通の再委託先から防衛庁データ流出。
- H15.6.26　ローソンから会員情報56万人分流出。
- H15.8.8　アプラスから顧客情報8万人分流出。
- H15.11.19　ファミリーマートから会員情報18万人分流出。
- H16.2.21　三洋信販から顧客情報最大120万人分流出のおそれ。
- H16.2.24　ソフトバンクBBから加入者情報451万人分流出。
- H16.3.9　ジャパネットたかた から顧客情報最大66万人分流出のおそれ。
- H16.3.19　シティバンク日本支店、顧客情報12万口座分、シンガポールで紛失。
- H16.3.25　アッカ・ネットワークスから顧客情報最大140万人分流出。
- H16.3.26　東武鉄道から顧客情報最大13万人分流出。

忍び寄る「高度情報漏えい化社会の影」

①大量化

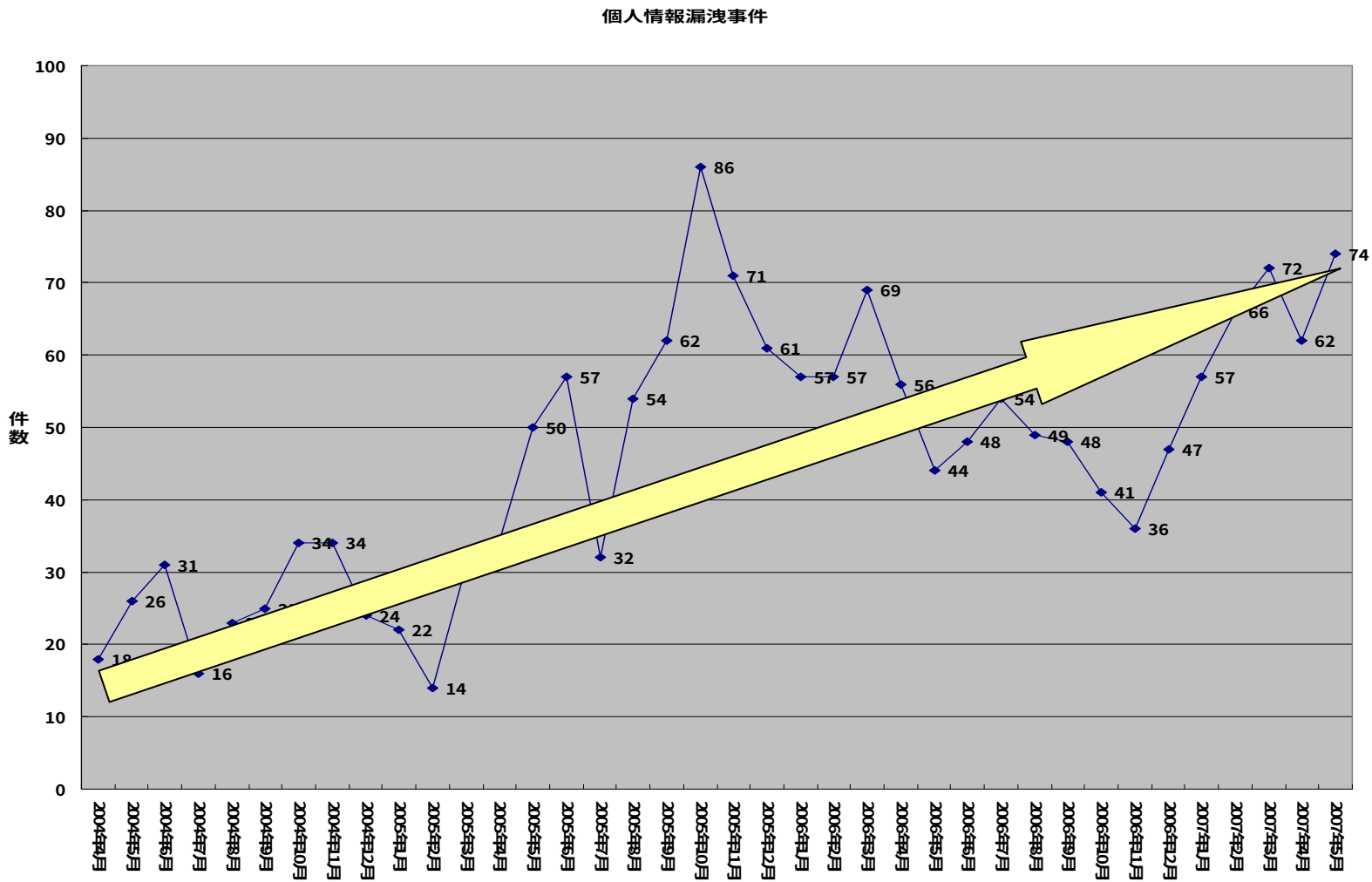
100万件を超える大量個人情報漏洩事件が続いています。

我が国で漏洩された個人情報の数が１００万件を超えたのは、２００４年2月の三洋信販事件です。それ以前は、１９９６年8月の全国信用情報センター事件の８３万件が最大でした。しかし、三洋信販事件以降は、堰を切ったように大量の個人情報漏洩事件が続いています（図表①）。５００万件を超える事件も、２００４年2月のソフトバンクBB、２００６年１２月の日産自動車と続き、今年3月には、大日本印刷事件で過去最大数を更新し８６４万件に達しました。このままでは、１０００万件超の漏洩事件もそう遠いことではないと思われます。

図表①１００万件を超える個人情報漏洩事件

流出件数	発生年月	企業･組織名
8,640,000	2007年3月	大日本印刷
5,380,000	2006年12月	日産自動車
4,000,000	2006年9月	富士ゼロックスシステムサービス
3,996,789	2006年6月	KDDI
1,760,000	2005年4月	札幌国税局
1,280,000	2005年4月	みちのく銀行
2,200,000	2004年4月	コスモ石油
1,400,000	2004年3月	アッカネットワークス
6,60,0000	2004年6月	ソフトバンクBB
1,160,000	2004年2月	三洋信販

個人情報漏洩事件報道件数の推移　(②件数増大)



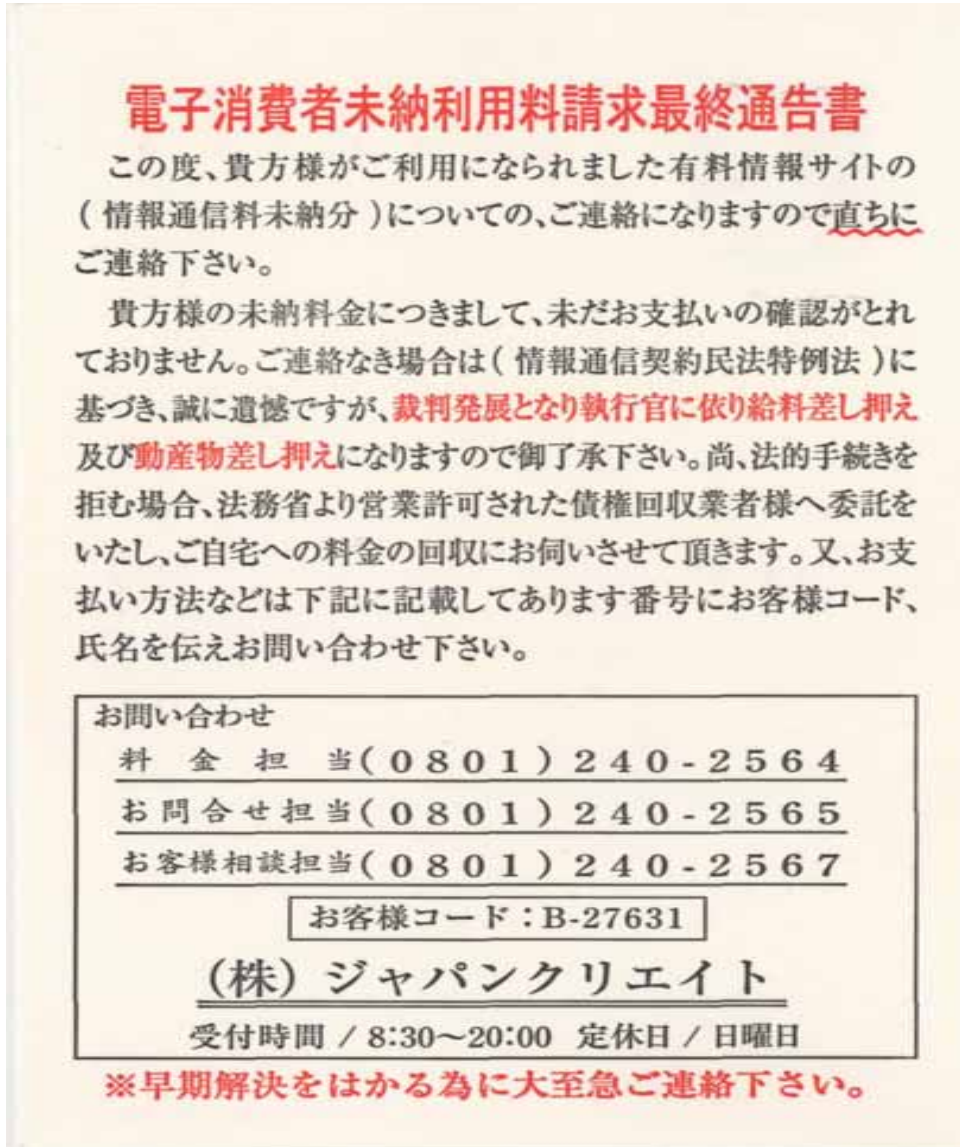
③漏洩形態の多様化　ウィニーによる情報漏洩の状況一覧　2005.4.1～2006.4.22

年	月	発見件数	漏洩情報件数、内容
2005	4	4件（官3）	2名～11255名の顧客情報（診療記録、消防情報含む）
	5	2件（官0）	603名の顧客情報、800件の携帯電話基地局情報
	6	4件（官2）	6名～535名の顧客情報（児童・教職員名簿、捜査報告書、人事考課情報含む）、原子力発電所の内部情報
	7	0件	
	8	1件（官0）	46カ所の原子力発電所の検査情報
	9	2件（官0）	137名の顧客情報、火力発電所技術資料
	10	2件（官1）	503名～564名の顧客情報
	11	7件（官3）	2名～3,544名の顧客情報、原子力発電所の報告書
	12	13件（官5）	3名～2,100名の顧客情報、空港制限区域の暗証番号、原子力発電所の技術資料
2006	1	10件（官6）	2名～30,000名の顧客情報（有権者名簿、医療患者情報、児童情報含む）、火力発電所資料
	2	22件（官17）	5名～3,609名の顧客情報（受刑者、捜査資料、患者情報、消防情報、生徒情報、裁判情報、検察情報含む）、海上自衛隊の機密情報
	3	48件（官20）	2名～13,619名の顧客情報（住基ネット情報、議員支援者名簿、性犯罪被害者名簿、従業員名簿、航空自衛隊隊員情報含む）、国内29空港のパスワード、社外秘内部資料、陸上自衛隊報告書、社内賭けゴルフ記録、市の業務メール
	4	22件（官6） （22日まで）	6名～127,053名の顧客情報（供述調書、前科照会書、児童・生徒・受験者情報含む）、米軍基地通行許可データ、国会議員への口利き文書、原発資料、皇太子ご夫妻の視察経路
		合計137件 （官63件）	注1　発覚件数欄の「（官N）」は、官公庁関係の件数（内数）を示す。 注2　漏洩情報内容欄の「顧客情報」には、個人情報と法人情報を含む。

ウィニー・リスクの整理・分析表

「護るべき情報資産」	社員の個人所有ＰＣで処理される企業の顧客情報や営業情報などの機密情報
「脅　威」	①　ウィニーがアンティニーというウィルスに感染しやすく、感染してしまうと、ウィニーが入っているＰＣ内の全てのファイルが交換用ファイルへコピーされてしまい、それによって、本人の知らない内に、ＰＣ内の全てのデータがＰ２Ｐで繋がったネットワーク内へ流出してしまうこと。
	②　しかもウィニーは匿名性の非常に高いＰ２Ｐのファイル交換ソフトであり、特定のサーバに拠らずにデータが配信されてしまうので、一度流出してしまったデータは現段階の技術では追跡・回収はほとんど困難になってしまうということ。
	③　さらにウィニーの利用者は現在約60万人くらいではないか、と言われているが、無料で簡単に入手利用でき、さまざまなコンテンツ（映画・音楽・ソフト・データなど）が無償で入手できる（著作権や営業秘密を侵害しているコンテンツも多いのであるが）ので、利用者は急速に拡大しており、社員の中にウィニーの利用者が増えている、ということ。
「脆弱性」	このようなウィニーの脅威に対して、企業として有効な管理策（コントロール）が取られていないこと。 具体的には、①ウィニーについての認識が不十分、②ウィニーについてのリスク分析が不十分、③ウィニーについての防止・抑制・検出・回復・管理というコントロール策の策定・実施が不十分、④特徴的には、社員の個人所有ＰＣによる企業情報処理に対するリスク対策が甘かったこと、など。
「リスク」	このような脆弱性が放置されていることによって、企業としてかなり機密度の高い情報資産が、知らない間に、広範囲かつ回収不能な状態で流出してしまい、それによって企業として、重大な社会的信用の低下や損害賠償の負担という経営的損失の危険があること。

架空請求はがき



電子消費者未納利用料請求最終通告書

この度、貴方様がご利用になられました有料情報サイトの（情報通信料未納分）についての、ご連絡になりますので直ちにご連絡下さい。

貴方様の未納料金につきまして、未だお支払いの確認がとれておりません。ご連絡なき場合は（情報通信契約民法特例法）に基づき、誠に遺憾ですが、裁判発展となり執行官に依り給料差し押え及び動産物差し押えになりますので御了承下さい。尚、法的手続きを拒む場合、法務省より営業許可された債権回収業者様へ委託をいたし、ご自宅への料金の回収にお伺いさせて頂きます。又、お支払い方法などは下記に記載してあります番号にお客様コード、氏名を伝えお問い合わせ下さい。

お問い合わせ

料　金　担　当（０８０１）２４０-２５６４

お問合せ担当（０８０１）２４０-２５６５

お客様相談担当（０８０１）２４０-２５６７

お客様コード：B-27631

（株）ジャパンクリエイト

受付時間／8:30～20:00　定休日／日曜日

※早期解決をはかる為に大至急ご連絡下さい。

「漏えい対策メニュー完備」それでも漏れた！
～「究極の」漏えい対策を求めて～

(1)「ＩＳＭＳ認証取得」「Ｐマーク取得」「対象者９割に研修実施」「ｅラーニング実施」
それでも、漏れた！

(2)「防止（客観的手段による漏えい機会の客観的減少）策」の徹底
①「三禁原則」－持たない・預からない・運ばない
②「セキュリティ区画」の徹底－注：「物理的区画」ではなく「論理ﾈｯﾄﾜｰｸ的区画」を
③「不可視性の克服」－「Ｐフラッグ」（存在の可視化）＋「ＰＩＴＳ」（ﾄﾚｰｻﾋﾞﾘﾃｨｼｽﾃﾑ）

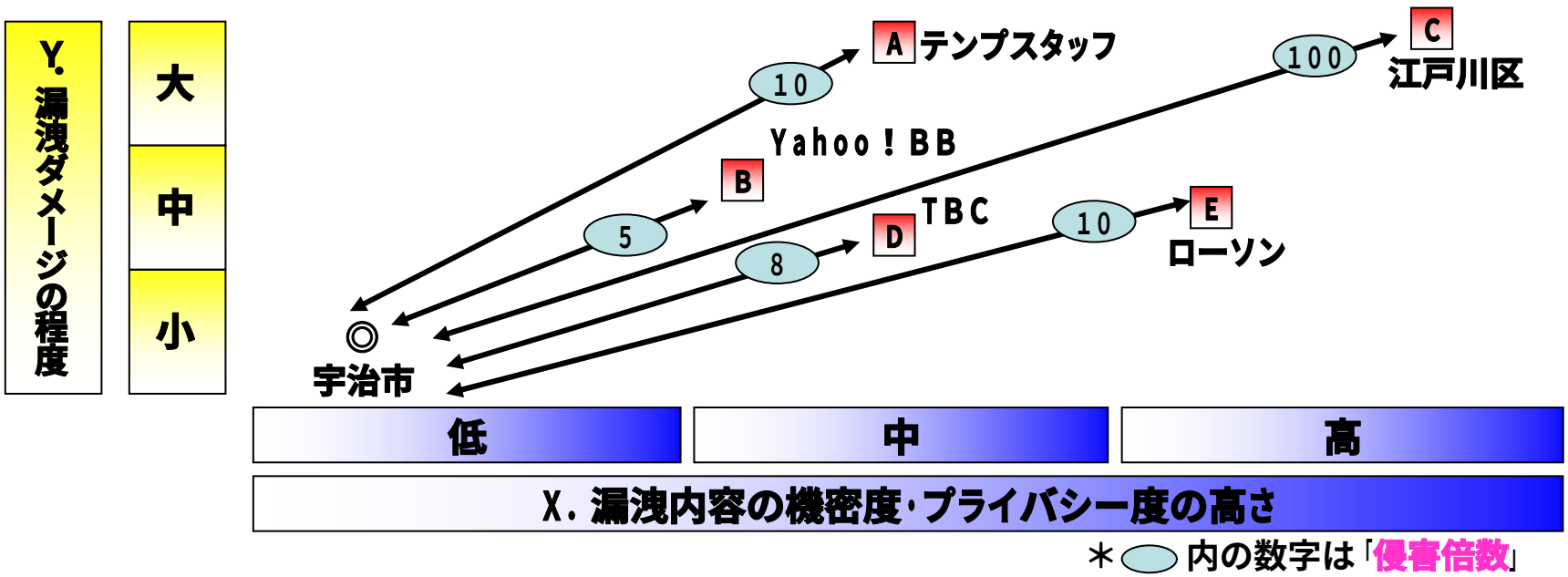
(3)「抑制（心理的抑圧により漏えい動機行動を抑制）策」の見直し・新構築
～単なるムチと単なる研修だけでは不十分－「故意」は抑制しても「過失－不注意」は抑制しきれない～
①業績拡大戦略における「魔」－セキュリティ戦略の不随伴→「拡大戦略だからこそセキュリティ」という「セキュリティ随伴戦略」のトップマネジメントにおける必要性
②異動変動による「すき間＝魔」→ルール・モラルの断絶
③「セキュリティ適性」による配置転換等の人事的統制
④「＋自制」の重要性－自律性・自主性・自発性
ⅰ．情報倫理の体系的管理的形成－「ＩＭＭＳ」(Information Moral Management System)
ⅱ．「汎用的教育・研修」から「問題解決実践」へ－「ＳＱＣ」(Security Quality Control)
ⅲ．社内セキュリティ資格制度の創設－ＩＳＭＳとの連動

(4)「新複合的漏えい対策」

【問題】 個人情報漏えいの損害賠償額

□貴方が、江戸川区の区民健康診断の情報漏えいの被害者だったとして、貴方が江戸川区に対して損害賠償を求めて国家賠償請求訴訟を提起したとします。裁判所はいくらの損害賠償を認めてくれるでしょうか。

＜損害賠償算定テンプレート方式＞



＊⬭内の数字は「侵害倍数」

情報漏洩事例のまとめ

	漏洩情報（推測を含む）	機密度	ダメージ	侵害倍数	賠償額（予測測定）
宇治市	基本情報のみ	低	小	1	1万円
Yahoo！BB	基本情報、メールアドレス、ID	中の下	中	5	5万円
テンプスタッフ	基本情報、非公開の携帯電話番号、美人度ランキング	中	大	10	10万円
江戸川区	基本情報、病歴	高	大	100	100万円
TBC	基本情報、セクシャルな事柄	中	中	8	8万円
ローソン	基本情報、電話番号、職業、年収、クレジットカードの番号	高の下	中	10	10万円

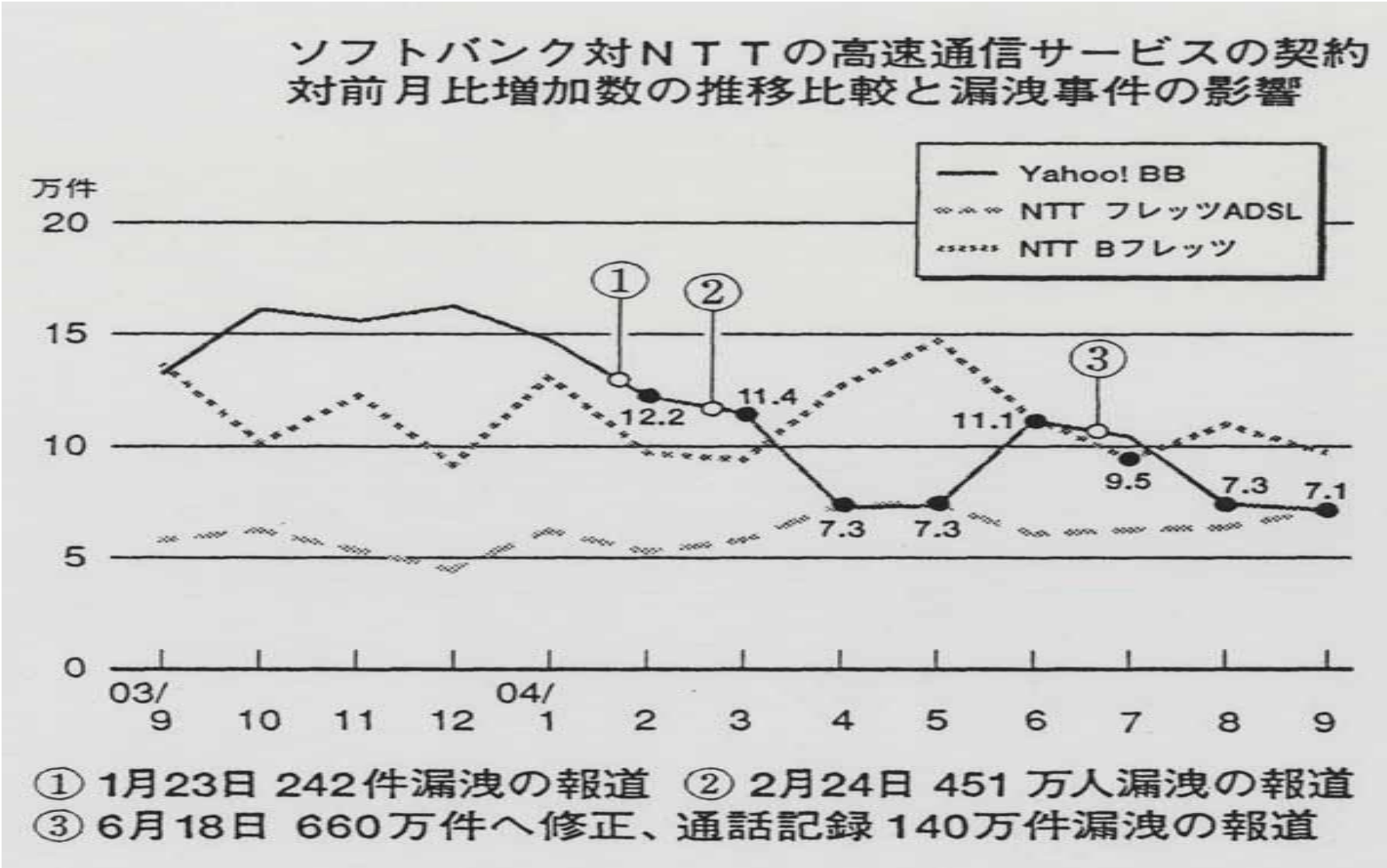
個人情報の種類

	漏洩内容の機密度･プライバシー度		
程度	低	中	高
区分	基本情報	取扱注意情報	センシティブ情報
意味	• 個人を特定するための基本的な情報 • 住民基本台帳に登録され制度的に公開が予定されている情報	• 機密度やプライバシー度が基本情報よりも高く、ある程度の高さの取扱注意を要する情報	• 機密度やプライバシー度が最高度に高く、その情報が知れることによって、社会的な不利益や差別につながる可能性を持つ情報
具体例	氏名 住所 生年月日 性別 イエローページ掲載の電話番号 ･ ･ ･ ･ ･	メールアドレス イエローページ不掲載の電話番号 携帯電話の電話番号 美人度ランキング 美容に関する相談内容 口座情報 クレジットカード番号 職業 年収 ･ ･	思想･信条･宗教に関する情報 歴史的社会的帰属情報 健康･病歴情報 多額債務情報 ･ ･ ･ ･ ･ ･

漏洩ダメージの程度

程度	
大	•二次流出、三次流出も起こり、回収は不可能 ▼ •漏洩データを使った侵害行為が発生した
中	•漏洩データが回収できていない ▼ •漏洩データを使った侵害行為は行っていない
小	•漏洩データがすべて回収された ▼ •漏洩データを使った侵害行為も起こらなかった

「社会的信用の低下」の金額的大きさ



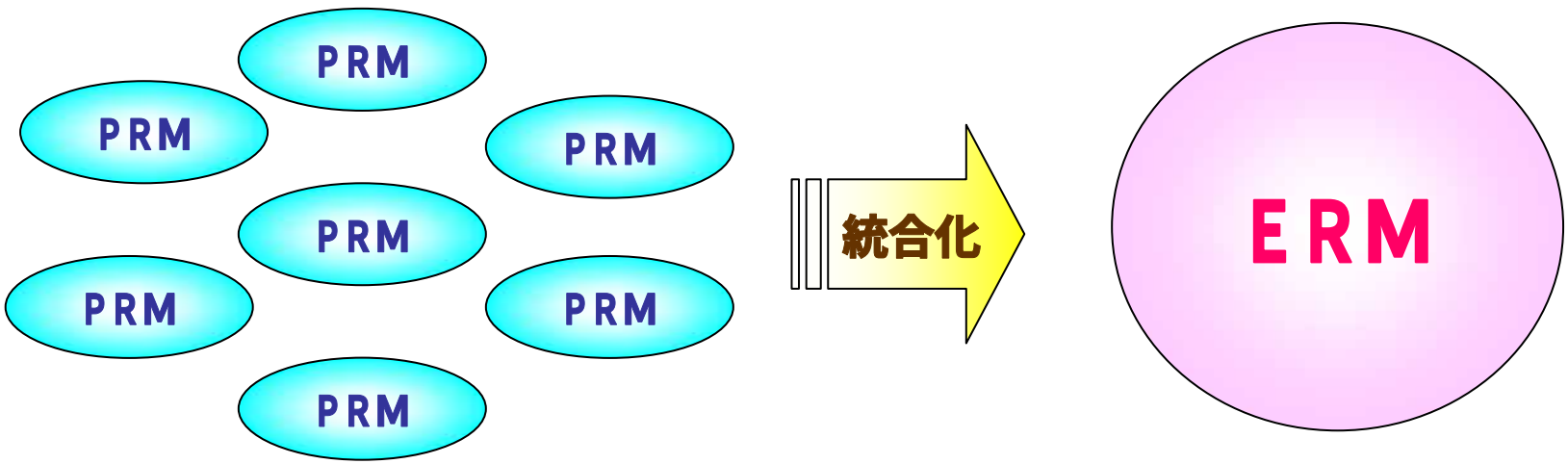
社員一人ひとりからの内部統制システムの整備

■「トップマネジメント」としての内部統制システム整備の重要性

■内部統制事故＝たった一人の職員の「0のかけ算」

■「社員一人ひとりからの内部統制システム整備への取り組み」が重要

PRM(ﾊﾟｰｿﾅﾙﾘｽｸﾏﾈｼﾞﾒﾝﾄ)からERM(ｴﾝﾀｰﾌﾟﾗｲｽﾞﾘｽｸﾏﾈｼﾞﾒﾝﾄ)へ



個人情報を保護する「こころ」の育成

- 平成16年7月、横浜市中区の産婦人科医が堕胎した**胎児の遺体**を「**一般ゴミ**」として捨てていた大きな社会問題になった。私たちは胎児の遺体の生々しさを瞬時に脳裏に描き、その悲惨さと医師に対するおぞましさを共感することができる。
- 平成16年9月、草加市役所からコンピュータ処理を受託した企業の元SEが、**市民の個人情報**が**印刷**されたテスト用**帳票**を「**一般ゴミ**」として捨てていて大きな問題になった。
- 草加市の事例を耳にしても私たちには、胎児の遺体の事例について感じたと**同じ感情が湧いてこない。なぜか。**テスト用帳票に印刷されていた市民の個人情報は、市民のプライバシー権＝**自己情報コントロール権＝人格権**、すなわち市民の「**こころ**」である。遺体と比べてこころが決して軽い訳ではない。しかし、私たち**人間という情報処理システム**（5感から入力される情報を脳で処理する）は、5感のうち「**目**」に**8割以上依存**している。そのため、**目に見えない「こころ」の大切さ**を理解するには**大変な努力**が**必要**なのである。
- ましてや、コンピュータのハードディスクの中に**デジタルデータ**として記録されている個人情報は、完全に「**不可視**」である。デジタルデータとしての個人情報のこころと向き合う私たちは、たとえてみれば**ヘレンケラー**のようなものである。私たちは個人情報のこころの大切さを理解するためには、その**三重苦**を乗り越えるための努力をしなければならない。
- 私たちの一人一人がこの困難さを認識し、**個人情報を保護する「こころ」を育む**ことが**究極の個人情報保護対策**なのである。

「企業情報(情報セキュリティ)管理法」概念図

企業情報(**情報セキュリティ**)管理法						物(物セキュリティ)管理法
企業情報(**情報セキュリティ**)管理原則:「最大活用性」「機密性・完全性・可用性」「説明責任性」「法適合性」						
取締法規 (社会秩序の保護)	役務・雇用	実体法(私人の情報に関する権利保護)			市場	物財産法
個人情報 利用調整義務	企業情報守秘・漏洩防止義務				経営情報 開示義務	
個　人　情　報			営業秘密情報	知的財産権情報	経営情報	
I	II	III	IV	V	VI	
個人情報保護法	委託契約・雇用契約 (就業規則・誓約書) の修正	民法 709条	不正競争防止法	特許法・ 著作権法	会社法・金融 商品取引法	
自己情報コントロール権と利用の便宜との調整①利用目的に関する義務②セキュリティに関する義務③開示・訂正等に関する義務	・個人情報保護法上の利用調整義務(公法的義務)の債務(私法的義務)化 ・個人情報漏洩防止義務(不法行為的義務)の債務(契約的義務)化	不法行為 損害の 事後救済	公正競争の 確保	無断使用の 防止	内部統制システムの整備・運用・評価(ERM)の義務化→内部統制報告書・内部統制監査報告書 ・株主代表訴訟	
行政指導・刑罰	損害賠償	損害賠償	刑罰・損害賠償	刑罰・損害賠償	刑罰・損害賠償	
本人(個人情報主)	委託者・雇用主	権利者	営業秘密権者	知的財産権者	株主・投資家等	**有体物所有主**
行政命令違反罪 ○	個人情報窃盗・横領罪× 不正アクセス禁止法○		情報窃盗・横領罪×、 不正アクセス禁止法○		**情報不開示・虚偽罪**　○	有体物窃盗・ 横領罪○