「個人情報保護法対策」から

「Ｊ－ＳＯＸ（内部統制ｼｽﾃﾑ整備）法対策」へ

～「セキュリティ」と「ガバナンス」と「法」～

「企業情報管理（セキュリティ）法」

２００６．２．１５

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

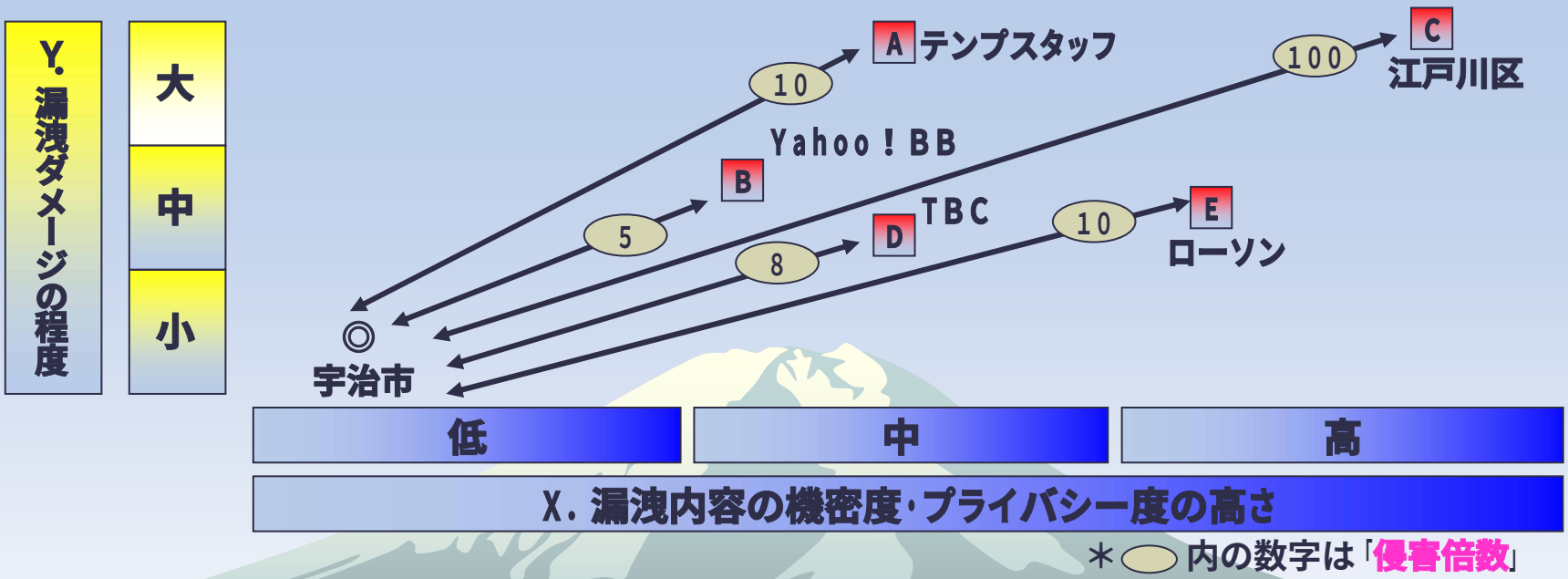
「企業情報(情報セキュリティ)管理法」概念図

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○

● 「情報セキュリティ法」とは、
「経営戦略においては、情報セキュリティ戦略が不可欠である」という考え方、および、
「経営者（取締役等）が、経営的意思決定において、情報セキュリティ注意義務を怠った場合には、法的責任を負う」という規範（ルール）のことをいう。

■情報セキュリティ注意義務を怠った事例
～ヤフーＢＢ事件～
■セキュリティ注意義務を怠った事例
～ＪＲ西日本福知山線事故～

＜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

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

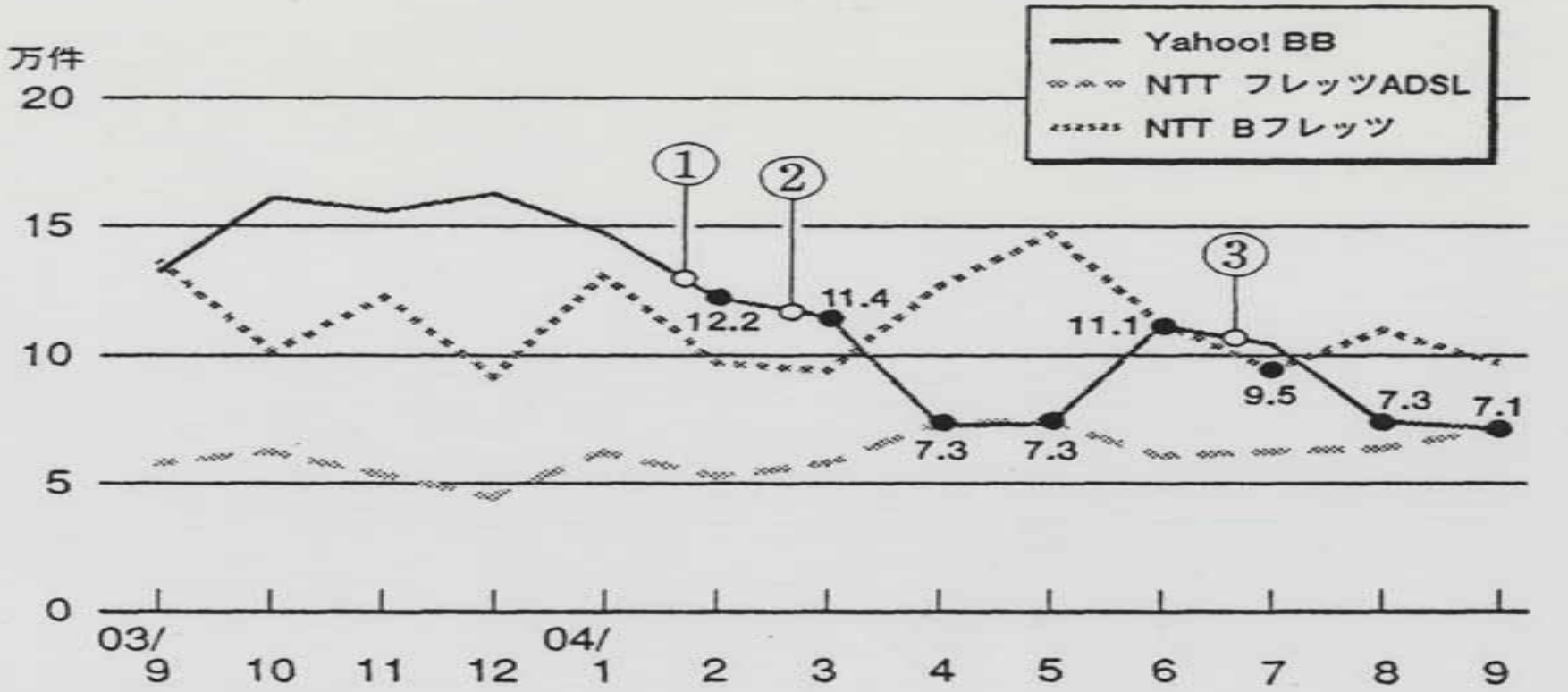
小

- 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



① 1月23日 242件漏洩の報道　② 2月24日 451 万人漏洩の報道
③ 6月18日 660万件へ修正、通話記録 140万件漏洩の報道

個人情報保護法制の概念図

個人情報保護法における「個人情報の種類」と個人情報取扱事業者

個人情報

生存する個人に関する情報であって、特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより、特定の個人を識別することができるようになるものを含む）。

個人データ

個人情報データベースなどを構成する個人情報

保有個人データ

個人情報取扱業者が、開示、訂正、追加または削除、利用の停止、消去、第三者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であって、政令で定めるもの。

個人情報取扱業者

個人情報データベース等を事業の用に供している者

- 15条〜18条・31条
- 15条〜23条・31条
- 15条〜31条・31条

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
～「自己情報コントロール権」を行使する機会保障の仕組み

		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	○
開示等	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	
	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		－	×
	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。

●個人情報保護法（個人法）における「セキュリティ規定」

第19条（データの正確性確保） 個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければならない。

第20条(安全管理措置) 個人情報取扱事業者は、その取り扱う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**を講じなければならない。
→①技術的措置・管理的措置＋②経営者の「内部統制不作為責任」明確化

第21条(従業員の監督) 個人情報取扱事業者は、その従業員に個人データを取り扱わせるに当たっては、当該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。
→①義務違反：行政指導、刑罰＋②使用者責任（民法715条）の監督義務明確化

第22条（委託先の監督） 個人情報取扱事業者は、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**を行わなければならない。
→ ①義務違反：行政指導、刑罰＋②使用者責任（民法715条）の監督義務明確化

●経営者の「内部統制（不作為）責任」

■H12.9.20 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。

■H15.4.5 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。

●「新会社法」における「内部統制システム」整備の義務化

■「取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制の整備」

◆会社法３６２条４項６号：取締役会の専決事項
同条５項：大会社である取締役会設置会社では、取締役会に決定義務
同法３４８条３項４号：取締役の専決事項
同条４項：大会社である取締役会非設置会社では、取締役に決定義務

●H15.6.27　経産省、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－」を公表。

●H17.3 経産省　「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」

1.2 現状認識（2）～IT事故を巡る社会情勢①国内

METI 経済産業省

コンプライアンスとCSR（Corporate Social Responsibility：企業の社会的責任）

- 平成17年４月１日の個人情報保護法全面施行により、個人情報取扱事業者に課せられる「安全管理措置」義務について、企業は早急な対応を求められている。
- 法令に基づく情報開示として①有価証券報告書におけるリスク情報の記載（証券取引法）、②金融業界のディスクロージャー誌におけるリスク管理体制の記載（事業法）がある。
- 社団法人日本経済団体連合会「企業行動憲章」では「社会的に有用な製品・サービスを安全性や個人情報・顧客情報の保護に十分配慮して開発、提供し、消費者・顧客の満足と信頼を獲得する。」との方針を示している。
- 企業のCSRに係る取組みを開示するCSR報告書でも、情報セキュリティ対策の方針や実施状況を採り上げる事例が出てきている。

個人情報の保護に関する法律（平成十五年法律第五十七号）

《抜粋》

（安全管理措置）
第二十条　個人情報取扱事業者は、その取り扱う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なければならない。

（従業者の監督）
第二十一条　個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該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。

（委託先の監督）
第二十二条　個人情報取扱事業者は、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わなければならない。

企業行動憲章（抜粋）

企業は、公正な競争を通じて利潤を追求するという経済的主体であると同時に、広く社会にとって有用な存在でなければならない。そのため企業は、次の10原則に基づき、国の内外を問わず、人権を尊重し、関係法令、国際ルールおよびその精神を遵守するとともに、社会的良識をもって、持続可能な社会の創造に向けて自主的に行動する。

（以下抜粋）
1.社会的に有用な製品・サービスを安全性や個人情報・顧客情報の保護に十分配慮して開発、提供し、消費者・顧客の満足と信頼を獲得する。

3.株主はもとより、広く社会とのコミュニケーションを行い、企業情報を積極的かつ公正に開示する。

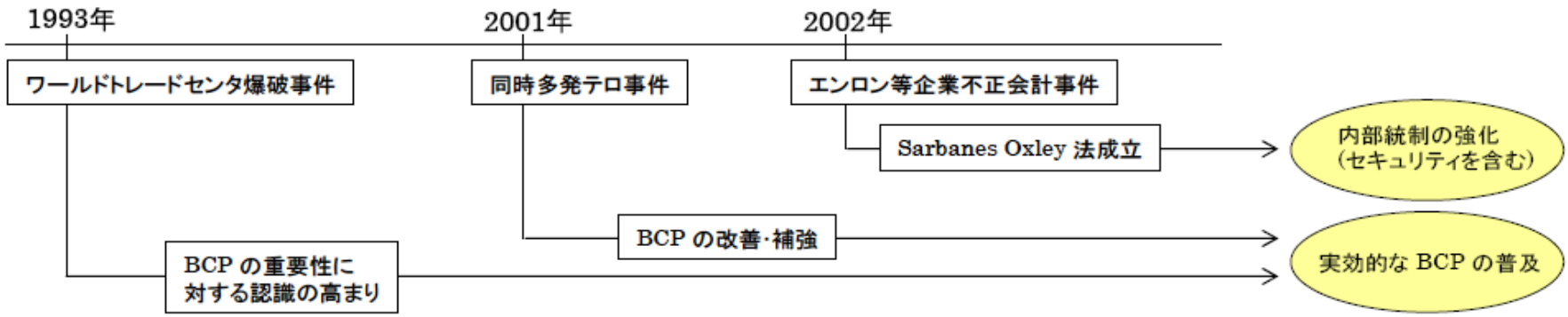
出所：（社）日本経済団体連合会，
「企業行動憲章― 社会の信頼と共感を得るために ―」
（2004年 5月18日改定）

1.2 現状認識（2）～IT事故を巡る社会情勢②米国

METI 経済産業省

米国では企業の不正行為やテロへの対策が情報セキュリティにも波及

- 米国では、不正会計事件を契機としたコーポレートガバナンスに対する法的規制の強化が、情報セキュリティ対策の取り組みにも影響。
- 事業継続計画（BCP）についても、2001年のテロ事件を契機に改善・補強する方向へ。



◆ Sarbanes-Oxley 法（2002年7月成立）

CEO および CFO が内部監査の結果について責任を負うことを規定し、コーポレートガバナンスの徹底を明確化した法律。
情報セキュリティ対策の徹底について直接言及はしていないが、法律に準拠するためには情報セキュリティ対策が必須となる。
IT との関連性が高いのは Section 404 であり、CEO･CFO･監査官に対して、会計報告書の作成プロセスが正確であることおよび一般的基準を満たすことを保証しなければならないと規定している。これによって企業は、会計報告書の作成に関わる全ての情報システムについて、法律が規定する基準を満たす事を保証しなければならなくなるため、結果的に情報セキュリティ対策を強化する必要に迫られることになる。

◆ その他のセキュリティ関連の法律

米国では、あらゆる業種を対象とした情報システムのセキュリティ強化を規定する法律は存在しないが、金融機関や医療保険業界といった特定の業界を対象として、情報セキュリティの強化を規定する法律が存在する。

- 金融業界：Gramm-Leach-Bliley Financial Modernization Act of 1999（GLBA）
  金融機関に対し、包括的セキュリティプログラムの策定やセキュリティ対策の実施を義務づけ。
- 医療保険業界：Health Insurance Portability and Accountability Act of 1996（HIPAA）
  個人の電子的な医療情報に対するセキュリティ対策の実施や電子署名の使用等包括的なセキュリティ対策の実施を義務付け。

2.1 情報セキュリティガバナンスの必要性

METI 経済産業省

企業のあるべき姿と政府の役割

- 高度にネットワーク化されたIT社会では、企業*1一社のIT事故によるトラブルが社会・経済全体にも影響する可能性。したがって、企業の情報セキュリティ確保は、自身の被害*2の局限化や法令遵守に留まらず、IT社会を構成する一員としての企業の責務といえるのではないか。
- 政府の果たすべき役割は、企業の情報セキュリティに対する努力を企業価値として評価するとともに、そうした取組みを促す環境の整備を支援することにあるのではないか。

情報セキュリティガバナンスの必要性

- 企業が、上記の「あるべき姿」に向かうためには、対策をその場しのぎの対症療法的対応で済ませるのではなく、自律的・継続的に改善・向上する仕組みを導入することが必要。
- つまり、社会的責任にも配慮したコーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること、すなわち「情報セキュリティガバナンス」の確立が求められる。
- ITの利便性を犠牲にするのではなく、利便性と安全・安心の両立を目指していくことが重要。

*1) 検討対象は主に情報システムの「ユーザ企業」。ただし、いわゆる重要インフラ業種（特に制御系）は、特別なリスクを有し、別途高いレベルのリスク管理策を検討する必要があると思われる。
*2) 株主等の損害も含む。

「情報セキュリティガバナンス」の確立
社会的責任にも配慮したコーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用する

政府の役割
企業の努力を企業価値として評価するとともに、そうした取組みを促す環境の整備支援

企業のあるべき姿
企業が自身の被害の局限化や法令遵守の観点に加え、社会的責任の観点も踏まえた形で情報セキュリティ対策に積極的に取り組む

OECDガイドライン
「セキュリティ文化」

情報セキュリティ総合戦略
「世界最高水準の『高信頼性社会』」

2.2 情報セキュリティガバナンスの確立に向けて

METI 経済産業省

問題

(1) IT事故発生のリスクが明確でなく、適正な情報セキュリティ投資の判断が困難
- ✓ 投資判断のための指標が求められているのではないか。

(2) 既存の情報セキュリティへの「対策」「取組」が企業価値に直結していない
- ✓ 情報セキュリティに係る取組みが、企業価値向上に寄与する仕組みが必要ではないか。

(3) 事業継続性確保の必要性が十分に認識されていない
- ✓ IT事故発生時の対応手続きを事業継続の観点から定めておくことが必要ではないか。

問題点を克服し、企業が情報セキュリティガバナンスの確立を促進するツール

情報セキュリティ対策ベンチマーク
- 情報セキュリティ対策のセルフチェック等に有用なベンチマークの指標を開発
- さらに、IT事故データ収集のあり方や被害想定額算出手法について調査し、ベンチマークデータと連動したリスク評価の可能性を模索

情報セキュリティ報告書モデル
- 企業のコンプライアンスや社会的責任を説明するIRの一環として、自らの情報セキュリティポリシーやそれを実現する対策の実施状況について対外的に公表する「情報セキュリティ報告書」を提唱し、そのモデル案を策定

事業継続計画策定ガイドライン
- 企業がIT事故発生時にも事業運営を継続的に維持するための事業継続計画(BCP)について、その策定手順や検討項目、事例等を紹介する「事業継続計画策定ガイドライン」を策定

企業・社会への普及方策
- ・情報セキュリティ格付け
- ・政府調達への活用
- ・損害保険との連携　　等

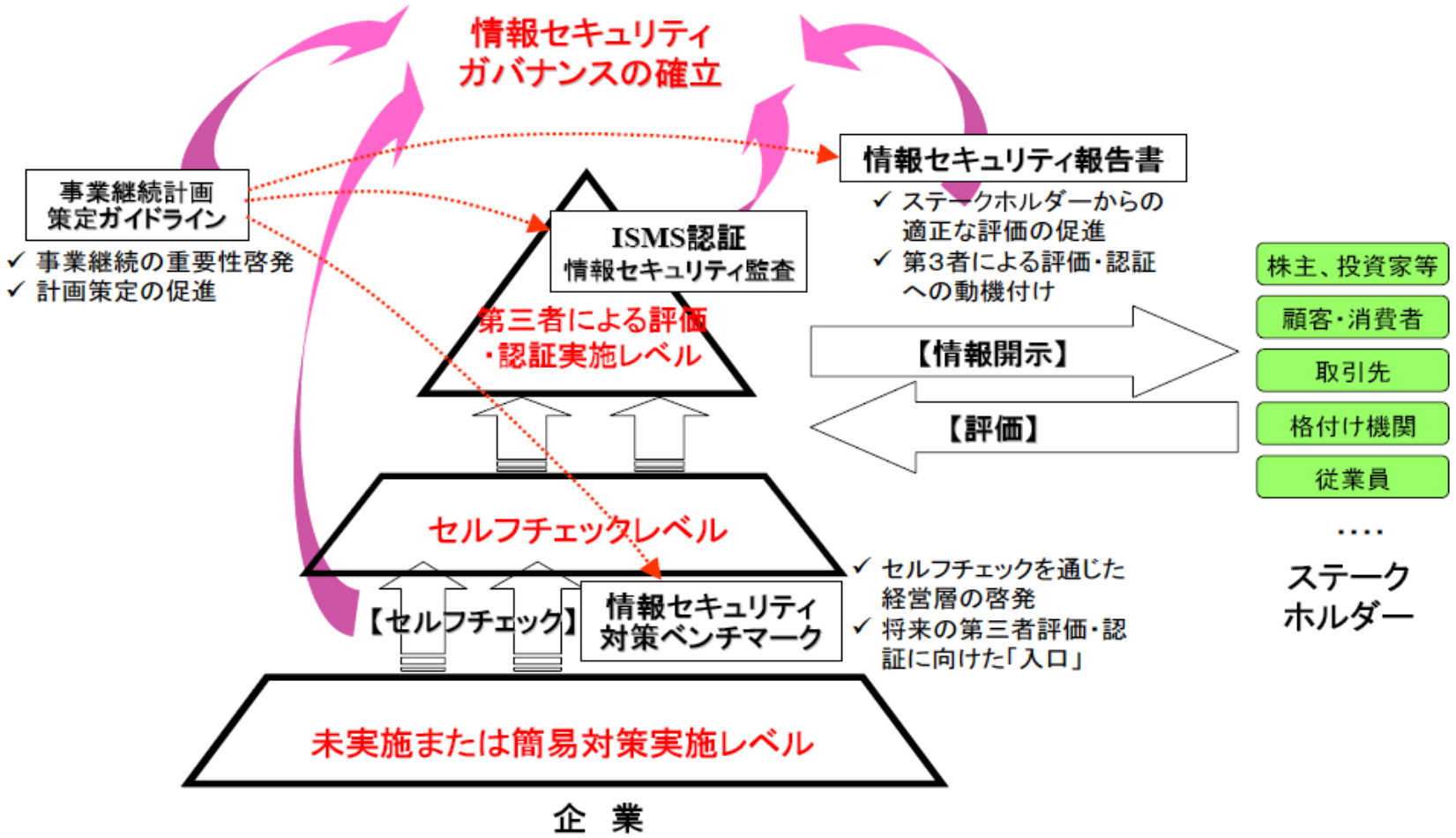
既存施策との連携
- ・ISMS認証や情報セキュリティ監査の「入口」としての活用
- （セルフチェック→第三者認証・評価へ）　等

企業における情報セキュリティガバナンスの確立

2.3 施策ツールとISMS認証等との基本的関係

METI 経済産業省

- 対策ベンチマークは、第3者評価・認証の実施へとつながる「入口」の役割を担う。
- 情報セキュリティ報告書は、情報開示をおける客観的な評価・認証の重要性を啓発する。
- 事業継続計画の策定は、ISMS認証等で評価される情報セキュリティ対策の強化や、情報セキュリティ報告書の充実に寄与する。



●国家社会的セキュリティガバナンス

■「セキュリティ事故」とは、
ある科学技術に対するコントロールミスにより、
その科学技術のデメリット（リスク）が顕現化することである。

■「科学技術を使うことを許す」とは、
科学技術のメリット（有用性）を実現する権利を付与する、だけでなく、
科学技術のデメリット（リスク）を帯有してよい、
セキュリティ事故が起こっても免責される、
「法的地位」を付与することである。

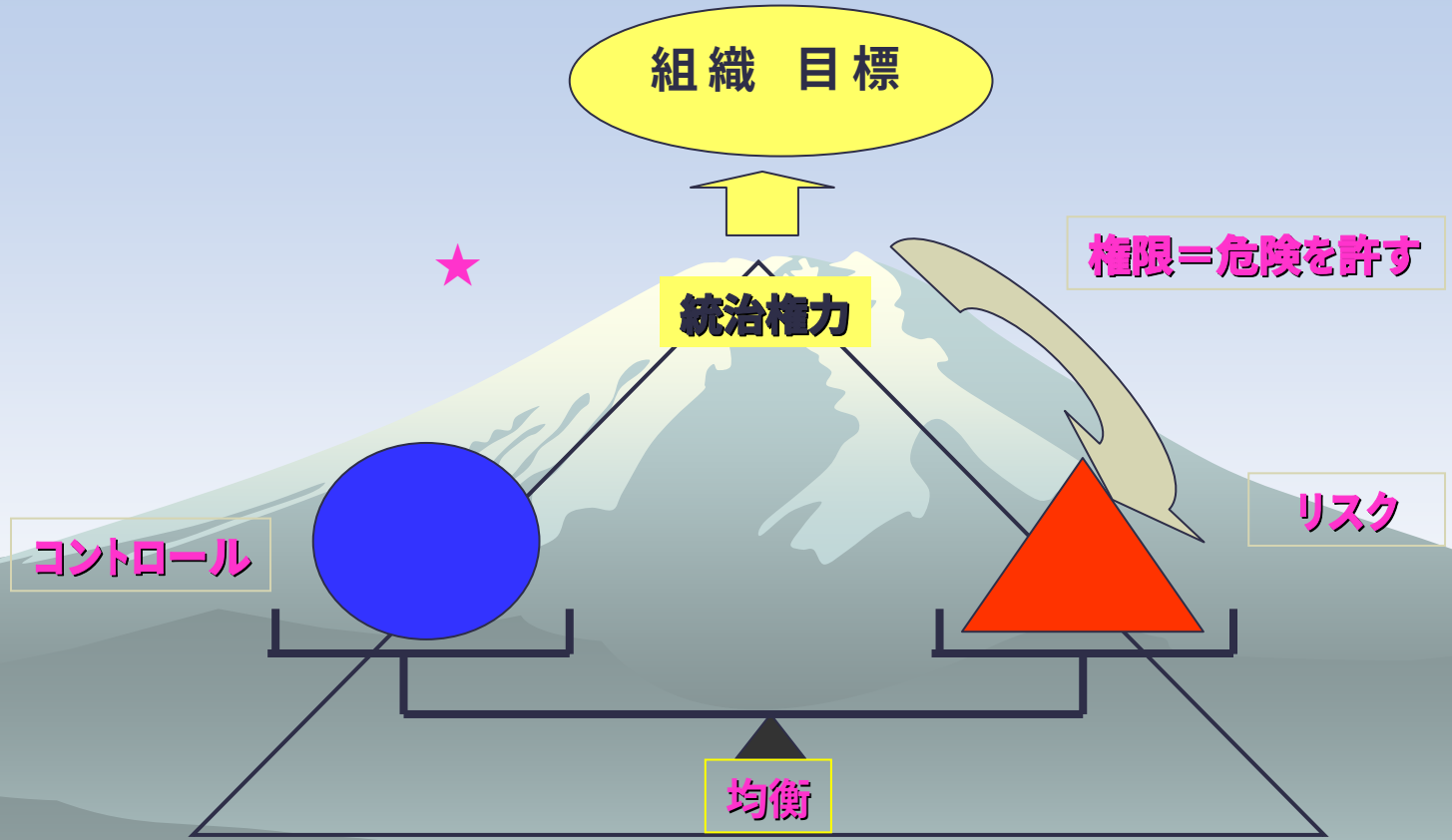
●国家社会が、科学技術の利用を許すのは、
「社会的危険を許す法理」に基づく。

■「社会的危険を許す法理」とは、
「ある科学技術の危険性が大きい場合でも、
その科学技術の利用によって得られる社会的
利益（社会的有用性）がより大きい場合には、
その科学技術の危険性をコントロールする技術・
手段が存在し、
そのコントロールが適正に行われることを条件として、
その科学技術の利用（それに伴う社会的危険）を許す」、
とする法的考え方である。

■「社会的危険」を「許す」とは、
万が一、その社会的危険が現実化してしまった（事故）場合でも、
コントロールの実施について、
注意義務を果たしていた場合には、
その事故についての民・刑・行の法的責任を問われない、ということである。

■「許す」のは、
主権者たる国民→民主的統治権力→国会の法律による。

●セキュリティに関する社会的統制原理



●「自動車」技術における「社会的危険を許す法理」
衝突事故によって、人の生命・身体の安全が
損なわれるリスク（平和な日本で1万人／年事故死）
がある。
しかし、自動車を使わなければ、食料・原材料
などを運送できず、生存・製造活動が損なわれるし、
人が移動できなければ、社会的活動が損なわれる。
■法的態度：原則的禁止の解除＝免許（許可）制度
・安全運転技術の習得による免許
・危険運転（例えば、飲酒）行為による免許取消・刑罰
★刑罰の強化による飲酒運転死亡事故の激減
　→リスクコントロールの成功

●「インターネット」技術における「社会的危険を許す法理」

インターネットにおける社会的危険

・個人情報漏洩
・ネット幼児買春
・ネット自殺

■法的態度：原則自由、必要性に応じて個別対応

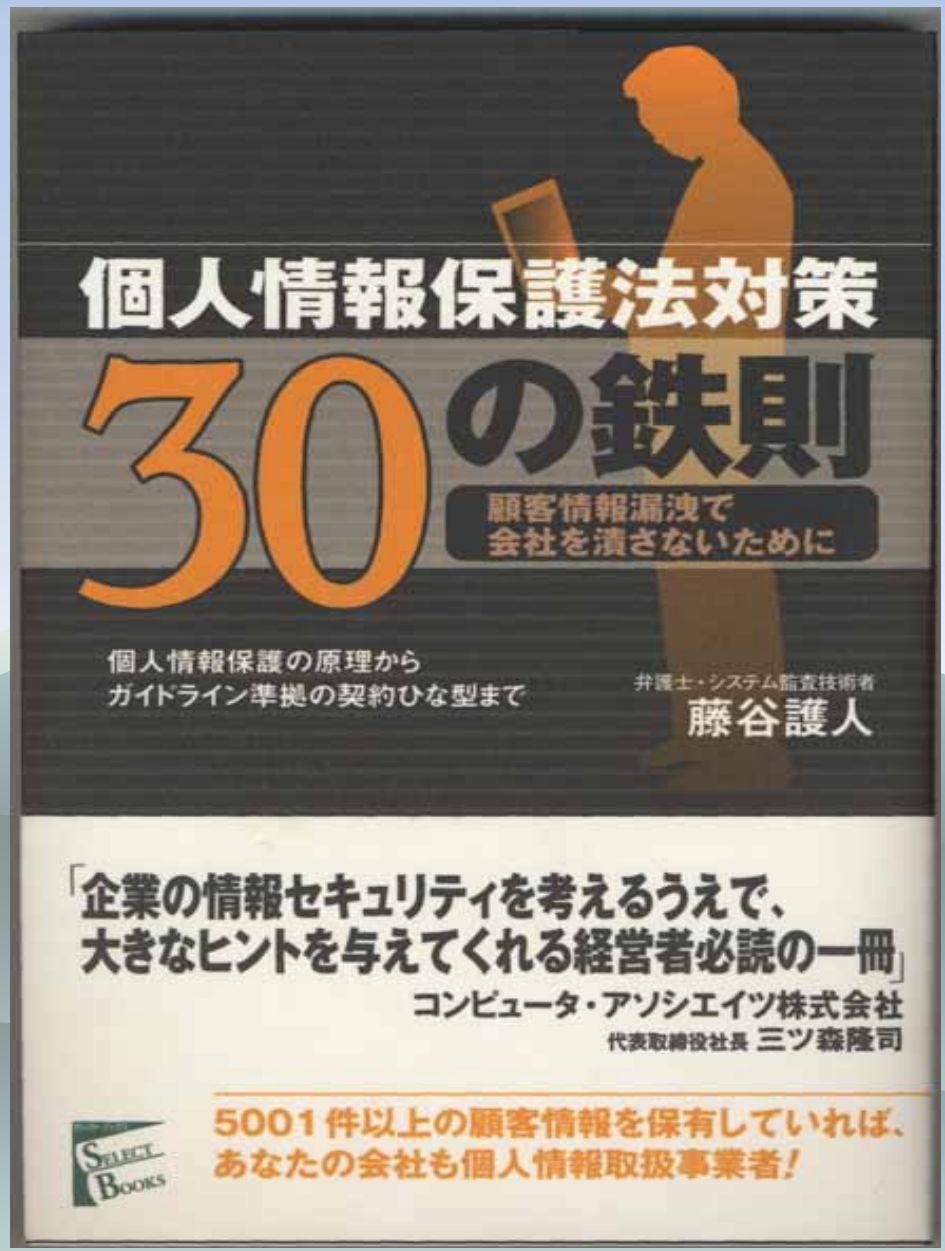
・個人情報保護法→漏洩防止法ではなく、利用調整法
・情報窃盗罪の規定がない→抑止力の欠如
・ネット幼児買春禁止法
・ネット自殺呼び掛けの監視

★　・・・・・→　未成功

●企業におけるセキュリティガバナンス
～企業における「危険を許す法理」～

■会社民主主義：許すのは「株主」

■社員が、リスクの保持を許されるのは、そのリスクの大きさと均衡のとれたコントロール（内部統制）の仕組み（ルール）を整備している場合のみ



ご清聴、ありがとうございました。

お問い合わせ先

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

藤 谷　護 人

〒101-0062 東京都千代田区神田駿河台２－５ 村田ビル8階
TEL 03-5217-5050 FAX 03-5217-5040
E-mail : fujitani@lt-law.jp